TM

RealNetworks

REALPROXY ADMINISTRATION GUIDE

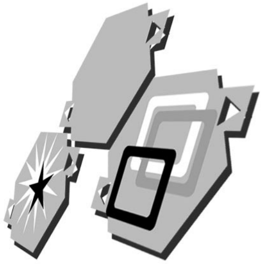
Version 8.0

RealNetworks, Inc.
2601 Elliott Avenue, Suite 1000
Seattle, WA 98121
U.S.A.

http://www.real.com
http://www.realnetworks.com

Printed in the United States of America.

CONTENTS



INTRODUCTION

Welcome to RealProxy™, a proxy server that works with RealPlayer® and RealServer™ to reduce streaming media bandwidth and to improve the viewing experience.

Overview

This manual is aimed at information services administrator who will be setting up and maintaining RealProxy.

How This Manual Is Organized

This manual contains the following chapters:

Chapter 1, Quick Start

Begin here for step-by-step instructions on getting RealProxy started and running quickly.

Chapter 2, “Overview”

This chapter gives the “big picture” of how RealProxy works.

Chapter 3, “Starting and Stopping RealProxy”

This is a guide to starting and stopping RealProxy. Options for starting RealProxy automatically, on different platforms are discussed. License information is given here.

Chapter 4, “Configuring RealProxy Features”

This chapter reviews RealSystem Administrator, the web-based console for fine-tuning RealProxy features.

Chapter 5, "Connecting Clients to RealProxy"

There are just a few steps you need to take to set up clients to take full advantage of RealProxy. Or, you can set up RTSP redirection so that this happens automatically.

Chapter 6, "Advanced Features"

This chapter discusses differences between RealProxy on the different platforms, the assignment of IP addresses for RealProxy's use, and some differences between RealProxy and RealServer.

Chapter 7, "Firewalls and RealProxy"

If you are delivering content to users on the Internet, you'll want to know how RealServer and other RealSystem™ products interact with firewalls.

Chapter 8, "Managing Bandwidth"

RealProxy has several methods of managing the amount of bandwidth it uses. You can limit the amount of bandwidth in use at one time, and place a cap on the number of clients who can receive streaming media.

Chapter 9, "Limiting Access to RealProxy"

Learn how to limit which clients use your RealProxy, based on their IP addresses.

Chapter 10, "Proxy Routing"

By employing several RealProxys at once, you can funnel all streaming media Internet traffic through a single point.

Chapter 11, "Multicasting Live Streams"

Take advantage of multicasting when streaming from RealProxy.

Chapter 12, "Authenticating RealProxy Users"

RealProxy authentication provides a way for you to control the sites visited by RealPlayer.

Chapter 13, "Monitoring RealProxy Activity"

To provide highest quality service, you'll want to keep track of how many people are accessing your RealProxy.

Chapter 14, "Tracking RealProxy Activity"

RealProxy can report player behavior with a customizable degree of detail. Errors are reported in their own log, which can help you troubleshoot any problems that arise.

Chapter 15, “Troubleshooting RealProxy”

If something isn’t working the way you expected, check here for ideas on finding out what’s happening.

Appendixes

Appendix A, “Configuration File Syntax”

This appendix consists of a discussion of the XML syntax used by the configuration file.

Appendix B, “Configuration File Contents”

This is a guide to the RealProxy configuration file, for those who prefer to edit it directly rather than using RealSystem Administrator.

Conventions Used in This Manual

Because this manual is aimed at the RealProxy administrator, the term “you” refers to the administrator.

RealSystem clients, such as RealPlayer, are referred to generically as “clients”. Where information applies specifically to the RealNetworks® RealPlayer or RealPlayer Plus™, this is spelled out. Although most clients in use are RealNetworks’ own RealPlayer, RealNetworks also makes a software development kit that enables other companies to develop their own players which can also receive streamed data types.

“Clips,” “content,” “media files,” and “files” are used interchangeably to indicate the material that RealProxy streams.

The following table explains the typographic conventions used in this manual:

Notational Conventions

Convention	Meaning
`syntax`	This font is used for syntax of configuration files, URLs, or command-line instructions.
`value`	Italic text represents variables. Substitute values appropriate for your system.
. . .	Ellipses indicate nonessential information omitted from the example.
[ ]	Square brackets indicate optional material. If you choose to use the material within the brackets, do not type the brackets themselves.

Additional RealSystem Resources

In addition to this manual, you may be interested in the following RealNetworks resources, available on the RealNetworks web site.

- General Information

  You can always read about RealProxy special offers at **http://www.realnetworks.com/products/proxy**.

- RealProxy Release Notes

  The release notes have the very-latest information about RealProxy, at **http://service.real.com/help/library/guides/proxy/readme.htm**

- *RealProxy White Paper*

  For a high-level look at how RealProxy can be used to best advantage on your network, review the white paper at: **http://service.real.com/help/library/whitepapers/proxy/proxy.html**

- *RealServer Administration Guide*

  The basic reference for the RealServer administrator, this manual explains how to set up, configure, and run RealServer to stream multimedia, available at **http://service.real.com/help/library/index.html**.

- RealSystem Software Development Kit

  RealNetworks has developed a Software Development Kit (SDK) that lets you integrate applications with RealSystem or create new plug-ins for RealServer or RealPlayer. Knowledge of programming is required to use the SDK. Register for and download the SDK from **http://www.real.com/devzone/**.

- Firewall Information

  You'll find information on using our products with firewalls at **http://www.service.real.com/firewall/**.

QUICK START

Once you have installed RealProxy, this chapter gives step-by-step instructions on putting RealProxy into production.

Overview

In this chapter, you'll use RealPlayer to first play content directly from a RealServer, and then you'll configure and use RealPlayer to go through RealProxy to get the same content.

Before you begin, you'll need the following software on your system:

- RealProxy
- RealPlayer (available for free download from **http://www.real.com**).
- A web browser

The software can be installed on different computers, but the computer on which RealPlayer is running needs a sound card and speakers (so that you can see and hear that all the software is working).

The steps for getting started are:

Step 1: Use RealPlayer to Play Content from a RealServer

Step 2: Start RealProxy

Step 3: Monitor RealProxy

Step 4: Configure RealPlayer To Use Your RealProxy

Step 5: Play Content Again

Step 6: Monitor RealProxy Again

Step 1: Use RealPlayer to Play Content from a RealServer

Using RealPlayer, test your network connection by playing sample content from a RealServer. You can use any of the following as sources for the test material:

- any channel listed in RealPlayer's Channel bar or menu
- clips streamed from your own RealServer
- sample content included in the free RealServer Basic (downloadable from **http://www.realnetworks.com**)

Make a note of which clips you played; you'll use this again later, to test RealProxy in Step 5.

Step 2: Start RealProxy

Common methods for starting RealProxy are listed below.

There are also other options for startup, and more details, described in Chapter 3, "Starting and Stopping RealProxy".

Windows NT Operating System

When you install RealProxy on Windows NT, by default it installs itself as a service, and runs automatically. If it isn't running, on the **Start** menu, click **Programs**, then click **RealProxy**, and finally click **RealProxy**. This starts the `rmserver.exe` program.

UNIX-Based Operating Systems

Move to the main RealProxy directory and type the following:

```
Bin/rmserver rmserver.cfg
```

If your RealProxy does not start, consult Chapter 15, "Troubleshooting RealProxy"

Step 3: Monitor RealProxy

Start RealSystem Administrator, the web-based console for configuring and monitoring your RealProxy, and use its Monitor to see that RealProxy isn't in use.

Tip

If you are using RealProxy on Windows NT, you can double-click the RealSystem Administrator icon on your desktop and skip the steps below.

➤ To start RealSystem Administrator:

1. Start a Web browser from anywhere on your network.
2. In the browser's address or location box, type the following URL, substituting your values for *address* and *AdminPort*:

   `http://`*`address`*`:`*`AdminPort`*`/admin/index.html`

   The setup program generates a random value for `AdminPort` if you did not supply one. If you're not sure what number to use, refer to "How do I figure out which port number to use for RealSystem Administrator?".
3. You are prompted for your user name and password. Use the same user name and password you created during setup.

   If you don't remember your user name or password, consult "How do I look up my user name and password?".
4. Click **OK**.

   RealSystem Administrator starts.
5. In the left-hand frame, click **Monitor**.

   The monitor page appears in the right-hand frame. Notice that all the numbers in the columns show a value of zero.

Step 4: Configure RealPlayer To Use Your RealProxy

RealProxy doesn't tell clients to contact it; you must explicitly configure clients to use RealProxy. Use the steps below to configure your RealPlayer to use your RealProxy.

➤ To configure RealPlayer:

1. In RealPlayer, select **View>Preferences**.
2. Select the **Proxy** tab.
3. Select the **Use PNA Proxy** checkbox, and type the IP address or host name of your RealProxy computer in the box next to it.
4. In the **Port** box, type `1090`.
5. Select the **Use RTSP proxy** checkbox., and type the IP address or host name of your RealProxy computer in the box next to it.
6. In the **Port** box, type `554`.
7. Click **OK**.

Step 5: Play Content Again

Now that RealPlayer is configured to always contact RealProxy, use RealPlayer to play the same content you used in Step 1.

Step 6: Monitor RealProxy Again

Look at the Monitor in RealSystem Administrator. The numbers are different, demonstrating that your RealPlayer is now sending its requests to RealProxy, rather than directly to the RealServer.

Chapter 2

OVERVIEW

This chapter describes how RealProxy works, and demonstrates the benefits of using RealProxy.

How RealProxy Works

RealProxy is software you install on a network or ISP gateway that aggregates and handles client requests for media streamed from RealServer. RealProxy reduces network traffic by eliminating redundant requests for streaming media.

RealProxy provides four main benefits:

- reduces bandwidth consumption by eliminating redundant data transmissions
- improves quality of user experience by distributing streaming media close to the user
- provides mechanisms for controlling inbound and outbound bandwidth parameters, thus securing bandwidth for other applications
- masks the IP addresses of the client software

Overview of the RealProxy Process

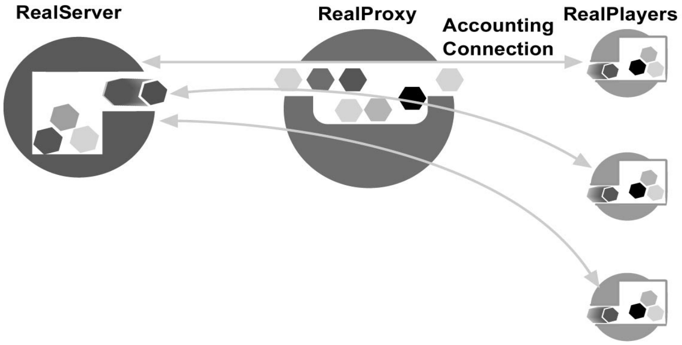
The first step in the RealProxy process happens when clients, such as RealPlayer, request streamed media files via RealProxy.

Next, RealProxy forwards the requests to the RealServer where the requested streamed media files are stored (called the "source RealServer").

RealServer verifies the file's existence, and that the clients are authorized through IP addresses or content authentication. If RealServer denies the request, it does not stream the requested file, and neither does RealProxy. Clients receive an error message.

This initial transaction, in which RealServer examines and authorizes individual client requests, is called an “accounting connection”, as shown in the following diagram.

Establishing the Accounting Connection

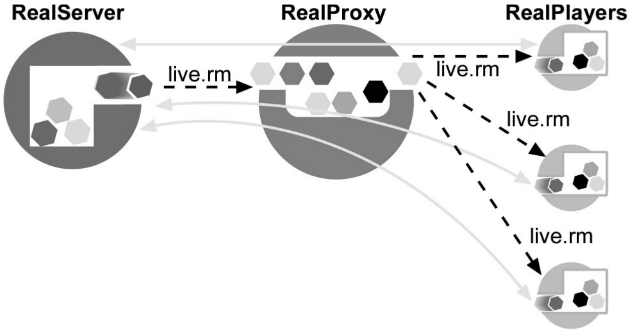


Depending on the nature of the streaming media, RealProxy uses different features to deliver the content to the client.

Delivering Live Streams

If the stream is live, RealProxy replicates the live stream for each client requesting the stream. The source RealServer sends only a single stream to RealProxy.

RealProxy Replicating Live Content



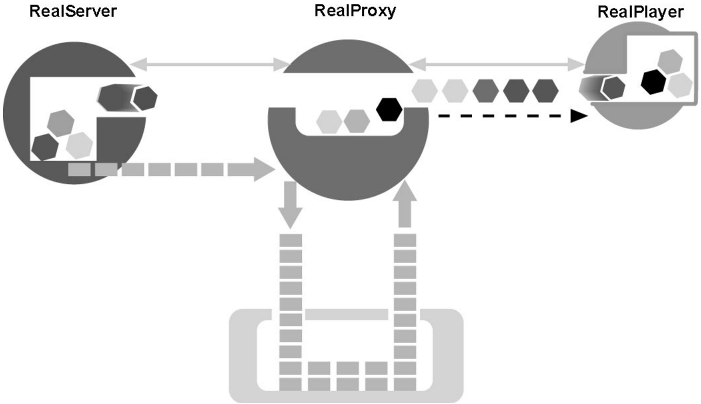
If the live stream is not available for replicating, RealProxy delivers the data separately for each client.

Delivering On-Demand Content

If the stream is on-demand, RealProxy first tries to fill the request from the media cache.

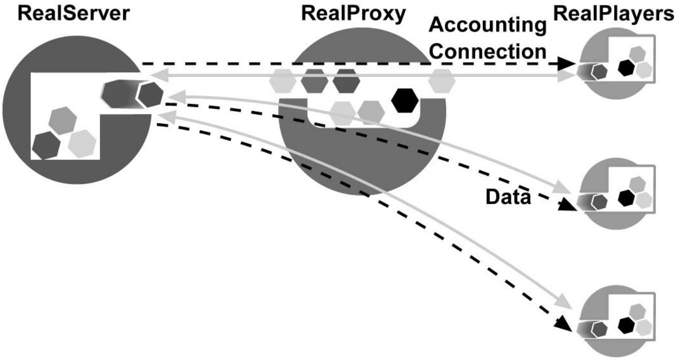
If the content is not yet stored in the cache, RealProxy will pull the content from the source RealServer, simultaneously serving the client and filling the cache.

RealProxy Streaming On-Demand Content from the Cache



If the stream is on-demand, and the clip is not cachable, RealProxy passes a data stream for each client that requested it, as shown in the following diagram.

RealProxy Streaming On-Demand Content (No Media Cache in Use)



A media cache file lowers network traffic by reducing the number of connections to the source of the requested material, and improves quality by distributing the streaming content closer to the user. Clients receive improved quality of service because media streams travel a shorter distance from the cache to clients, reducing the possibility of network congestion or packet loss.

RealProxy Features

RealProxy has three different ways of sending data to clients. RealProxy automatically chooses the most efficient feature possible, based on the type of content requested and the network configuration. The three methods are:

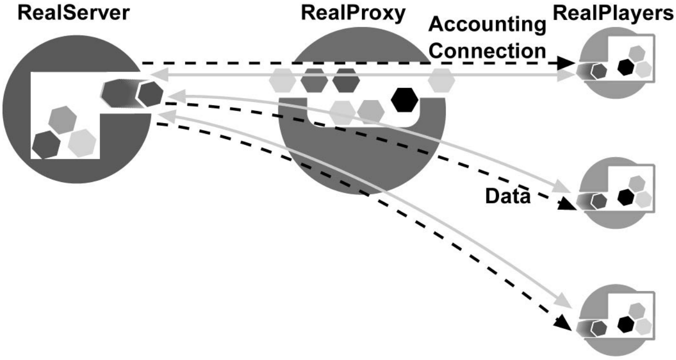
- **Passthrough** No bandwidth conservation is in effect, but all streaming media (both on-demand and live) requests go through RealProxy.
- **Pull Splitting** For live requests, RealProxy "shares" the stream among the clients who request it.
- **Cache** For on-demand requests, RealProxy stores the streaming media data for later viewing by other clients.

In addition, you can configure passthrough and pull splitting to transmit to clients via multicast. Regardless of the feature in use, RealProxy always opens an accounting connection between the client and the source RealServer.

Passthrough

This is RealProxy's simplest method of operation. In addition to the usual accounting connection opened between the client and the source RealServer, RealProxy creates a data connection for each client. No bandwidth conservation is appreciated.

Passthrough (for Live and On-Demand Streams)

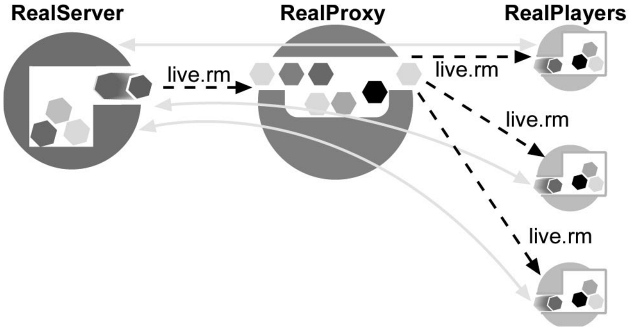


Pull Splitting

Pull splitting conserves bandwidth for live material. The first time a client requests a particular stream, RealProxy contacts the source RealServer on the client's behalf and then sends the stream to the client. The second client to request a live stream will receive it directly from RealProxy, and RealProxy will not have to obtain another stream from the source RealServer.

The advantage to the client is that the material is delivered from a nearby RealProxy. As long as the quality of reception for the single split channel between RealProxy and the source RealServer is sustained, RealProxy will receive a high-quality live stream, as well.

Pull Splitting (for Live Streams)



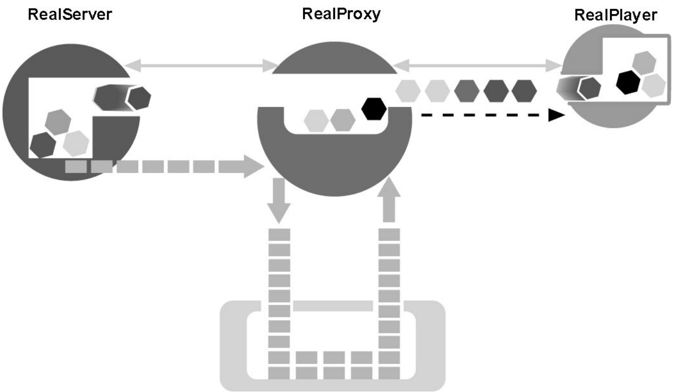
Cache

Cache software stores on-demand content from source RealServers. Since cached files are stored in a proprietary format and cannot be accessed directly, RealProxy interfaces with the cache to redistribute the stored media to clients.

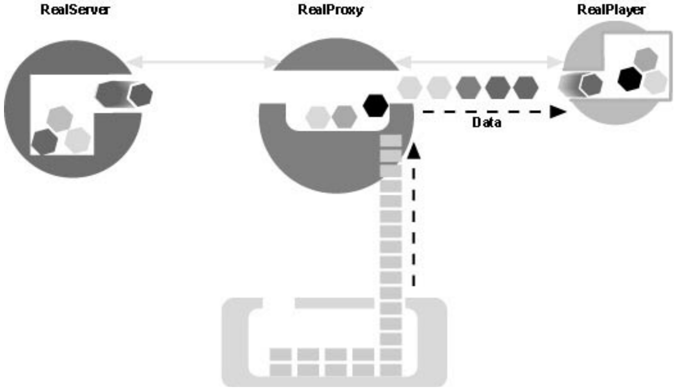
When caching is enabled, the media cache acquires and stores media files when requested by the first client. When a second client makes a request for a stream, RealProxy checks with the cache to see if a stored version is already present. To ensure that the stored version is the most up-to-date version available, RealProxy checks with the source RealServer to see if a newer version exists. After determining that the stored copy is the latest version, RealProxy streams the stored copy to the second client, and to subsequent clients that request the same material.

Only on-demand files streamed by RealServer 7.0 or later can be cached. Live material is handled as in the most efficient mode suitable—pull splitting or passthrough (and sent via multicast, if available on the network).

Filling the Media Cache with On-Demand Clips



Serving On-Demand Clips from the Cache



To ensure high-quality data at all times, RealProxy monitors the quality of both the cached media it is streaming and the connection between the source RealServer and the client. Should the media in the cache become impaired in some way, the stream halts and clients receive an error message. Or, if the accounting connection between the client and the source RealServer is interrupted, RealProxy terminates the stream, and the client receives an error message.

If a source RealServer has been configured to prevent caching, RealProxy will use the passthrough feature to deliver content to clients, without caching the media. When RealServer is installed, all its streams are cachable by default. Since RealServers can reach more clients if caching is allowed, operators are encouraged to leave all content cachable.

Requirements for Each RealProxy Feature

The following table outlines the configuration requirements for each aspect of RealProxy operation. In addition, RealProxy can be configured to use multicasting (where available) for those clips delivered in pull splitting mode. For more information, see Chapter 11, "Multicasting Live Streams".

Requirements for Each Feature

Feature	Special RealProxy Configuration	Your Network Requirements (assumes RealProxy is running)	Source RealServer Requirements
Passthrough	None.	None.	Broadcasting live and/or on-demand content.
Pull splitting	None. RealProxy is configured to do pull splitting by default.	Network allows UDP transport between RealProxy and RealServer. If only TCP is allowed, change RealProxy to use TCP.	Broadcasting live content. Configured to allow pull splitting, with default values. (RealServers are configured this way by default.)
Caching	None. RealProxy is configured to cache by default.	None.	Has on-demand content, and is configured to accept requests from caches. (RealServers are configured this way by default.)
Multicasting	Configured to use multicast address range. RealProxy uses pull splitting to deliver clips.	Clients and routers are multicast-enabled.	Broadcasting live content.

Compatibility with RealServer Versions

The method that RealProxy uses to distribute streams can depend on the version of the RealServer where the streaming media originates. For more details, refer to the table below.

RealProxy Compatibility with RealServer Versions

RealProxy Feature	RealServer Version Number		
	8.0, 7.0	G2 (6.0)	5.0 and earlier
Passthrough	Yes	Yes	Yes
Pull splitting	Yes (RTSP only)	Yes (RTSP only)	No
Caching	Yes	No	No

Additional Features

RealProxy contains additional features that make it easy to configure, administer, and maintain.

Administration

RealSystem Administrator is a web-based console for customizing RealProxy features. You can access via a browser anywhere on your network, using either Netscape Navigator version 4.06 or higher, or Internet Explorer version 4.0 or higher.

Changes you make using RealSystem Administrator are stored in the RealProxy configuration file. This text file is based on Extensible Markup Language (XML) and can be edited directly. Because the structure of this file is complex, RealSystem Administrator is the recommended tool for making changes.

See Chapter 4, "Configuring RealProxy Features" for specific instructions on customizing RealProxy.

Setting Up Clients

Once you have configured RealProxy, you will need to arrange for clients (such as RealPlayer) to send their requests to RealProxy.

There are two ways you can do this:

- Configure clients to directly contact RealProxy with their streaming media requests. You can send instructions for doing this to users. Refer to Chapter 5, "Connecting Clients to RealProxy".
- Configure RealProxy to intercept client requests. This does not require any special client configuration, but it does require the use of software or hardware which routes TCP traffic by destination port (such as a layer-4 switch). Consult your switch manufacturer's documentation for details.

Limiting Network Traffic

To limit the amount of bandwidth used by RealProxy, several features allow you to restrict the number of requests or amount of bandwidth it uses. Clients that attempt to contact RealServers after RealProxy's limits have been reached receive an error message.

Additional Information

See Chapter 8, “Managing Bandwidth”.

Proxy Routing

For organizations that use strict rules to regulate Internet traffic, proxy routing allows you to further control network traffic. With this feature, you can configure RealProxy to direct its clients’ requests to yet another RealProxy.

Additional Information

See Chapter 10, “Proxy Routing”.

Monitoring RealProxy in Real Time

RealSystem Administrator includes a Monitor which dynamically displays the status of your RealProxy.

Additional Information

Refer to Chapter 13, “Monitoring RealProxy Activity”.

Tracking RealProxy Activity

RealProxy records information in the access log about all clips it has served. Errors are noted in the error log.

RealProxy error logs use the same format as RealServer error logs. Access logs are similar to RealServer logs, but include additional information about the address of the source RealServer and the RealProxy operational mode (pull splitting, caching, and so on).

Log files on the source RealServer do not show that a RealProxy is in use; only the client data is gathered.

Additional Information

Access and error log information is described in depth in Chapter 14, “Tracking RealProxy Activity”.

Interaction with RealServer

This section describes what happens on the source RealServer when RealProxy forwards a client request.

Additional Information

If you are working with both RealProxy and RealServer, you may be interested in "Administering Both RealProxy and RealServer".

Controlling Client Access

Each time it receives a request, RealServer determines whether it can allow a particular client to receive streams, based on the number of available streams and bandwidth. In addition, RealServer may be configured to require a user name and password for certain material. If the requested material requires a password, the user will be prompted for the password. RealServer does not begin streaming until it receives the correct password.

Only after RealServer has authorized the client's request will RealServer begin streaming. Restrictions imposed by the source RealServer's administrator on client access are always honored by RealProxy. The same is true when a cache is in use—RealProxy waits for RealServer approval of each request before streaming it from the cache.

Denying Client Access

A source RealServer may deny a request for the following reasons:

- The requested material is secured, and the user does not have permission to access it
- RealServer can restrict access according to IP address, and the client's IP address or the RealProxy's IP address is on the restricted access list
- No more connections are available on the source RealServer. The number of connections is governed by the license, and can be further limited by the manager of the RealServer.

The client receives a message if it is denied access for any reason.

Tracking Activity

To the source RealServer, requests made via RealProxy appear identical to requests made by any other client, and information about quality of service is logged in the log file, just as it is for any other type of connection. Information about quality of service comes from the accounting connection.

Cache Requests

RealProxy only streams media from the cache after opening an accounting connection to the source RealServer. If the accounting connection cannot be established, or if it is disrupted, RealProxy will not stream from the cache to the client.

RealProxy cannot cache content which a source RealServer administrator has configured as non-cacheable. Instead, it will use passthrough mode to deliver the material to the client.

When RealProxy Will Not Conserve Bandwidth

Under the following circumstances, RealProxy will be unable to conserve bandwidth:

- If the source RealServer is configured to only allow caching on some files, or not at all. You have no control over this. (For example, a RealServer administrator might prevent frequently updated material, such as advertisements, from being cached.)
- If the source RealServer is not configured for pull splitting. If the RealServer is not set up to allow pull splitting, this mode won’t work.

In all cases, however, using RealProxy on your network serves to collect all streaming media traffic at a single point, so that you can better monitor activity and maintain security.

Protocols, Transports, and Packet Formats

RealProxy handles client requests and proxies RealServer streams by using the Real Time Streaming Protocol (RTSP), an Internet standard control protocol for streaming multimedia, and PNA, the RealNetworks legacy protocol. Although RealServer can stream via HTTP, RealProxy is not an HTTP protocol proxy and thus does not handle any streaming media requests made via HTTP between clients and a source RealServer.

RealProxy works with connecting RealPlayers to determine the best transport to use for a given stream: IP multicast (for live broadcasts), or UDP and TCP (for both live and on-demand content).

Data types streamed by RealServer and RealProxy use two primary packet formats: RDT, a proprietary packet format native to RealSystem, and RTP, an Internet standard data type packet format.

The following table outlines the protocols, transports, and packet formats supported by RealProxy.

Supported Protocols and Data Packet Formats

Control Protocol	Control Transport	Data Packet Format	Data Packet Transport	Supported by RealProxy?
RTSP	TCP	RDT (RealNetworks)	IP multicast, UDP, TCP	Yes
	TCP	RTP		
PNA (RealServer 5.0 and earlier)	TCP	RDT (RealNetworks)	UDP, TCP	Yes
	TCP	RTP		
HTTP (Streaming)	TCP	—	—	No
HTTP (Cloaking)	TCP	RDT (RealNetworks), RTP	TCP	

Additional Information

For details on the control transports and data packet transports allowed on each port, see Chapter 7, “Firewalls and RealProxy”.

Chapter 3

STARTING AND STOPPING REALPROXY

This chapter gives information on starting and stopping RealProxy on both Windows and UNIX-based platforms, and explains the RealProxy license method.

Windows NT

Instructions in this section describe how to start and stop RealProxy running under Windows.

Starting RealProxy Under Windows

RealProxy can be started manually or as a service. You can configure each service to use different configuration files.

Starting RealProxy Manually

You can start RealProxy from the **Start** menu or from a command line.

➤ To start RealProxy from the Start menu:

On the **Start** menu, click **Programs**, then click **RealProxy**, and finally click **RealProxy**. This starts the `rmserver.exe` program. If this is the first time you have run RealProxy, it loads the default configuration file.

Additional Information

The configuration file is described in Chapter 4, “Configuring RealProxy Features”.

➤ **To start RealProxy from a command line:**

Move to the RealProxy `Bin` directory and type the following at a command line:

```
rmserver ..\rmserver.cfg
```

Setting Up RealProxy as a Service

RealProxy on Windows NT can be run as a service. An option during setup configures this automatically. Instructions in this section describe how to add RealProxy to the services list if you did not instruct setup to do so.

You can load different configuration files into different Windows NT registry keys, and connect them to different instances of RealProxy running as separate services. Multiple services of RealProxy can be useful if you want to switch between a production and a test configuration file, for example.

➤ **To install RealProxy as a service:**

1. At a command prompt, move to the RealProxy `Bin` directory.
2. Import the configuration file you want to use into a specific key in the registry by typing the following:

   ```
   rmserver.exe -import[:key] configuration_file
   ```

   where:

   key is the Registry key name you want to use. If you omit it, the default name `Config` is substituted.

   configuration_file is the path and configuration file you want to import. For example, the following command:

   ```
   rmserver.exe -import:Proxy1 ../rmserver.cfg
   ```

   imports all the values in the `rmserver.cfg` file into the following key of the Windows registry:

   ```
   HKEY_CLASSES_ROOT\Software\RealNetworks\RealProxy\2.0\Proxy1
   ```

   Note

   You must supply the path to the configuration file. If RealProxy cannot find the configuration file, it will not start.

   Tip

   You can now start RealProxy using this configuration by typing the following at a command line:

   ```
   rmserver.exe registry:Proxy1
   ```

3. Install the service by typing the following command at a command prompt:

```
rmserver.exe -install[:ServiceName] "parameters"
```

where:

ServiceName is the name that will appear in the Services dialog box. If you omit *ServiceName*, `RMServer` is the default name.

parameters is either the name of the configuration file, or the registry and key name, as entered in Step 2. The format of the registry and key name is `registry:`*key*.

Note

The quotation marks surrounding *parameters* are required.

The next time you start RealProxy from the Services dialog box, it will use the settings specified in *parameters*, and will be configured to start automatically.

For example, the following command:

```
rmserver.exe -install:NewYorkProxy "Proxy1"
```

installs RealProxy with the service name "NewYorkProxy" and uses the settings in the Proxy1 key.

➤ To remove any RealProxy from the services list:

At a command prompt, type the following:

```
rmserver.exe -remove[:ServiceName]
```

where *ServiceName* is the optional name of the service. If you omitted a service name when you installed the service, you can omit it here, and RealProxy will use the default name `RMServer`.

Running Multiple RealProxys on One Windows NT System

You can have configuration files with different names for different configurations of a single RealProxy, or use different names for different RealProxy installations.

You can load configuration files into separate registry keys. Then, run RealProxy as a service, one for each configuration file you loaded.

➤ To import a configuration file into a specific key in the registry:

1. Follow the instructions in Step 2 of "Setting Up RealProxy as a Service".

2. Start RealProxy by typing the following:

   ```
   rmserver.exe registry:key
   ```

   where:

   key is name you want to use for the configuration. RealProxy places the configuration information in `HKEY_CLASSES_ROOT\Software\RealNetworks\RealProxy\2.0\Key`.

   In the example from Step 2 of "Setting Up RealProxy as a Service", in which the configuration settings are loaded into the "Proxy1" key, the full key name would be `HKEY_CLASSES_ROOT\Software\RealNetworks\RealProxy\2.0\Proxy1`.

Stopping RealProxy Under Windows

If RealProxy was started from the Start menu or the command prompt, switch to the command window and press **CTRL+C**.

If RealProxy was started as a service, stop RealProxy through the Services control panel.

UNIX

Instructions in this section describe how to start and stop RealProxy running under UNIX.

Starting RealProxy Under UNIX

Start RealProxy initially with the default configuration file; later, you can create other configuration files and start RealProxy using those.

➤ To start RealProxy under UNIX:

Run the `rmserver` program. It is located in the `bin` subdirectory of the RealProxy directory, and the configuration file (`rmserver.cfg`) is located in the main RealProxy directory.

Move to the `bin` directory and type the following:

```
rmserver ../rmserver.cfg
```

You can run RealProxy in the background by typing the following from the `bin` directory:

```
rmserver ../rmserver.cfg &
```

If you have other configuration files, you can substitute their names for `rmserver.cfg` and RealProxy will use the settings in the file you name.

➤ To limit RealProxy's memory use:

To limit the amount of memory that RealProxy uses, start RealProxy with the `-m` parameter:

```
rmserver ../rmserver.cfg -m 32
```

where the number after `-m` can be any amount of memory in megabytes, 32 or greater. Each megabyte of RealProxy memory accommodates 3 to 4 simultaneous connected users. To allow 200 users to connect, specify 50 megabytes of memory instead of 32.

Stopping RealProxy Under UNIX

There are two ways to stop RealProxy under UNIX: with a keystroke and with the kill command.

You can press **CTRL+C** to stop RealProxy.

To use the kill command, first obtain the process identification number, and then issue the **kill** command with that process number. The process ID is stored in the `rmserver.pid` file, which is usually kept in the `Logs` directory. The `PIDPath` variable specifies this location.

You can perform both actions with one command. Move to the directory which contains the RealProxy PID file, and type the following:

```
kill 'cat pidfile'
```

where *pidfile* is the name of the RealProxy `PID` file, as shown in the `PIDPath` variable. The usual name for this file is `rmserver.pid`.

License Information

The number of client connections available to your RealProxy is determined by information in the license file.

If your RealProxy suddenly allows only 25 connections (rather than the licensed number of 10,000), either your license has expired or RealProxy is unable to start using the settings you've selected. If your license file is incorrect or has expired, contact RealNetworks for a correct license file.

Reading the License File

You can read the file with RealSystem Administrator by clicking **About** in the left-hand frame. A second browser window appears, displaying the values for your license file. If you have multiple license files, RealProxy will show the values for all of them at once.

You can also read the file with any text editor.

Warning

Do not edit the license file. Any modification to the license file will render it invalid, and RealProxy will not start.

This file is written in XML format and is stored in the license directory.

The `LicenseDirectory` variable in the configuration file tells RealProxy where to look for license information. This variable can only be changed by editing the configuration file directly. To learn about the configuration file, see "Configuration File".

Chapter 4

CONFIGURING REALPROXY FEATURES

All RealProxy settings are customized through the RealSystem Administrator. This chapter describes how to use RealSystem Administrator as well as the basic settings used by all RealProxys.

Customizing RealProxy Using RealSystem Administrator

RealSystem Administrator is the Web-based console for customizing RealProxy features. It can be run from any browser on your network. It is password-protected when first installed, and you can create additional user names and passwords for any other people who will be helping you administer your RealProxy.

When the RealProxy installation program completes, it asks if you want to run RealSystem Administrator. If you choose yes, RealProxy starts, and RealSystem Administrator displays.

To make changes to any feature, click on the appropriate category listed under Configure. Make the changes and click Apply. A confirmation page appears to let you know that the changes have been made. You may be required to restart RealServer; a message to that effect will appear if it is necessary.

If your Web browser is set to permit cookies, RealSystem Administrator "remembers" the page that was open in the right-hand frame the last time you used it or when you click the refresh button. In Netscape Navigator, RealSystem Administrator will reload with the main Welcome page when you resize the browser window unless cookies are enabled.

Note

RealProxy must be running before you can use RealSystem Administrator.

Starting RealSystem Administrator

You can view the configuration of your RealProxy from nearly any browser on your network. Compatible browsers are Netscape Navigator version 4.0 or higher and Microsoft Internet Explorer version 4.0 or higher.

➤ To start RealSystem Administrator:

1. Start RealProxy. (See Chapter 3, “Starting and Stopping RealProxy” for instructions).
2. Click the browser shortcut created by the RealProxy installer, or use the following instructions:

   In a browser, type the following address:

   `http://`*`realproxy.example.com`*`:`*`AdminPort`*`/admin/index.html`

   where:

   `realproxy` is the name of the machine on which RealProxy is installed.

   `example.com` is the name of the domain in which RealProxy exists.

   Or, rather than typing the name and domain of the system on which RealProxy is installed, you can type the IP address.

   `AdminPort` is the port which RealSystem Administrator uses to connect to RealProxy. You are asked for a port number during setup. Use that port number here.

   The following URL will start RealSystem Administrator if it is typed in the browser on the same computer as RealProxy (be sure to substitute your port number for *`AdminPort)`*:

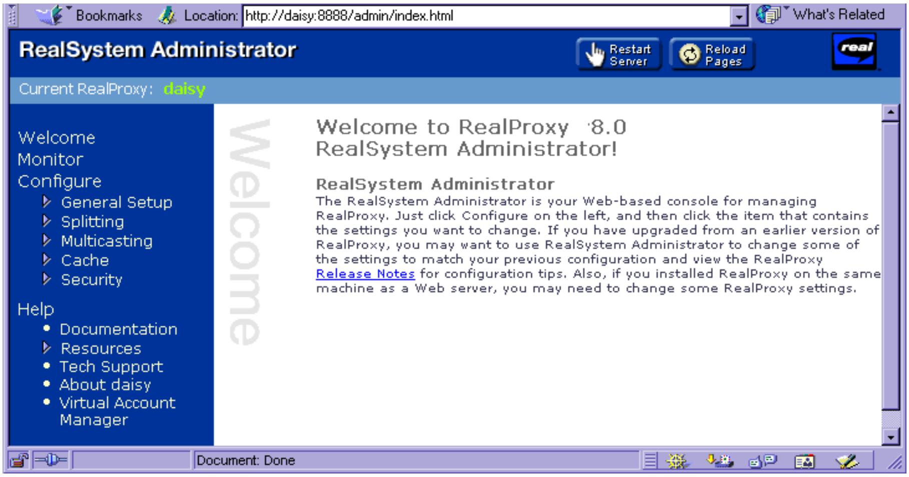
   `http://127.0.0.1:`*`AdminPort`*`/admin/index.html`

   The following command also works on the same computer:

   `http://localhost:`*`AdminPort`*`/admin/index.html`
3. You are prompted for your user name and password; these will match the values you entered during setup. Click **OK**.

   RealSystem Administrator appears.

RealSystem Administrator Welcome Page



Welcome to RealProxy 8.0 RealSystem Administrator!

RealSystem Administrator

The RealSystem Administrator is your Web-based console for managing RealProxy. Just click Configure on the left, and then click the item that contains the settings you want to change. If you have upgraded from an earlier version of RealProxy, you may want to use RealSystem Administrator to change some of the settings to match your previous configuration and view the RealProxy Release Notes for configuration tips. Also, if you installed RealProxy on the same machine as a Web server, you may need to change some RealProxy settings.

Using RealSystem Administrator

Once you have started RealProxy and then RealSystem Administrator, you can change RealProxy features with the instructions below:

➤ To customize RealProxy settings:

1. In RealSystem Administrator's left-hand frame, click the appropriate category below **Configure**.
2. Change the values in the page on the right.
3. When you have finished changing values, click **Apply**.

   RealSystem Administrator makes the changes to the configuration file.

   For some changes, RealSystem Administrator may alert you that you need to restart RealProxy using the **Restart Server** button at the top of the screen.

Restricting Access to RealSystem Administrator

When you install RealProxy, RealSystem Administrator is configured to require user names and passwords for anyone who connects to RealSystem Administrator itself. You can add permission for additional users, so that other people in your organization can use RealSystem Administrator to customize RealProxy.

Additional Information

RealProxy uses a subset of the authentication features available to RealServer. For more information on authentication, refer to *RealServer Administration Guide*.

➤ To add access for additional RealSystem Administrator users:

1. In RealSystem Administrator, click **Security**. Click **Realms**.
2. In the **Authentication Realms** list, select `SecureAdmin`.
3. In the Realm User Management area, click **Add a User to Realm**.

   A new dialog box appears.
4. Type the new user name in the **Name** box.
5. In the **Password** box, assign a password.
6. Retype the password in the **Confirm Password** box.
7. Click **OK**. A message appears; click **Close**.

Repeat Step 2 through Step 7 for each person who will have administration privileges.

Tip

You can verify that the users were added successfully by clicking **Browse Users in Realm**. A new browser window appears, displaying the names of all the users.

Configuration File

Changes made with RealSystem Administrator are stored in the configuration file. There are a few specific features which can only be adjusted by editing the configuration file directly. These are highlighted in “Features Only Available Via Direct Editing”.

The configuration file is a text file formatted with tags which are based on XML (Extensible Markup Language). This language introduces great flexibility to the configuration file format and allows third-parties to use this file and add to its functionality. Syntax of this file is given in Appendix A, “Configuration File Syntax”.

Be sure that your configuration file is stored where only authorized users can make changes to it.

Tip

Keep a backup copy of the configuration file. You may need it if you make changes to this file that you later want to undo or if you accidentally delete the working copy.

Editing the Configuration File with a Text Editor

You can change the RealProxy settings by opening the configuration file with any text editor. You can also add variables that aren't included in the initial file, but are listed in this manual in Appendix B, "Configuration File Contents". In addition, third-party plug-ins may require their own parameters and variables. Use a text editor to add them to the configuration file.

To make changes to existing settings in this file is simple; this manual provides guidance. If, however, you plan to add new sections, you will need to understand the syntax of the entire file. The file is organized into sections. This is not strictly necessary, but helps with clarity. The structure of the configuration file is described in detail in Appendix A, "Configuration File Syntax".

The default name of the configuration file is `rmserver.cfg`, but if you have multiple servers you may want to rename the files so as to easily identify which server you're working with.

When you edit the configuration file manually, be sure to use correct syntax, because RealProxy looks for exact spellings and correct use of angle brackets. RealProxy does not display messages related to syntax errors; instead, it will ignore those settings it does not understand.

Note

Always restart RealProxy after changing any settings in the configuration file with a text editor.

RealSystem Administrator shows the configuration file settings of the RealProxy configuration file in use; use caution if you are switching between manually editing the file and using RealSystem Administrator to edit it.

Warning

Exit RealSystem Administrator before opening the configuration file with a text editor or unexpected changes may result.

Common Settings

Regardless of which features are in use, certain important settings apply to every RealProxy. They are described in this section.

Port Variables

Port settings tell RealProxy where to listen for requests.

If your RealProxy and Web server are on the same machine, you may need to modify the HTTP Port setting. See “Running Web Servers and RealProxy on the Same System” for additional information.

RealProxy uses the following settings to determine where to listen for requests sent via a particular protocol. You can view the settings from RealSystem Administrator by clicking **General Setup>Ports**.

- **PNA Port**—the port where RealProxy listens for material requested via PNA (these begin with `pnm://`). The default value is `1090`.
- **RTSP Port**— the port where RealProxy listens for RTSP requests (these begin with `rtsp://`) At installation, the value is `554`.

Note

To use a port lower than 1024 on a UNIX system, you must be logged on as super-user.

- **Admin Port**—port number to which RealSystem Administrator connection requests are directed. The value for this setting is selected at random during setup to ensure security, and can be overridden by the user during setup.

There are other settings on this page, and they are described elsewhere in this guide. See Chapter 10, “Proxy Routing”.

Configuring RealProxy Features

To customize RealProxy features, you’ll need to modify settings with RealSystem Administrator or by editing the configuration file directly. But all of RealProxy’s features are enabled by default; there is no need to set up any features.

Passthrough

Passthrough mode is always enabled. It can’t be turned on or off.

Media Cache

The media cache is enabled by default. You do not need to make any changes to begin using the cache automatically.

The cache feature uses the following settings, which are pre-configured:

- **Enable Caching**—the feature is set to `Enabled` by default.
- **Maximum Cache Size**—This is the largest the cache will grow before removing Least Requested URLs (see “Changing the Size of the Cache” below). The default value is 1000 megabytes.
- **Cache Directory**—The directory location of the main cache file structure. The default directory is `Cache`.

Changing the Size of the Cache

Once the cache has reached its maximum size, RealProxy removes the media which were requested the least often. This method is called Least Requested URL.

> **Tip**
> It’s a good idea to make the cache size as large as you can, since the more you can cache, the more bandwidth you can conserve.

➤ To change the size of the cache:

1. In RealSystem Administrator, click **Cache**. Click **Cache** again.
2. In the **Maximum Cache Size** list, type the largest size you want the cache to reach, in megabytes. (The default value is 1000 megabytes. The minimum value you can use is 11 megabytes.)
3. Click **Apply**.

Pull Splitting

When a client requests a live stream, RealProxy checks to see if the transmitter RealServer is configured for pull splitting. RealProxy then gets the live stream using the highly efficient pull splitting connection.

Pull splitting is enabled by default.

RealServer uses the following settings to perform pull splitting (you can view them by clicking **Splitting>Pull Splitter** in RealSystem Administrator), and they are pre-configured:

- **Mount Point**—the mount point you will use in the URL for split content. The default value is `/split/`.
- **Port**—the port number on the transmitter RealServer to which the splitter will direct its requests. The default value is 3030.
- **Protocol**—indicates the protocol to use in sending live data to splitters. The default is `UDP`. Choose `TCP` if you are splitting through a firewall (this may produce a slower connection with more overhead).

Multicasting

Instructions on configuring RealProxy to perform multicasting are located in Chapter 11, “Multicasting Live Streams”.

Chapter 5

CONNECTING CLIENTS TO REALPROXY

For client software (such as RealPlayer) to contact and use your RealProxy, you either explicitly configure the clients to connect to RealProxy, or use an L4 switch or router to automatically direct client requests to RealProxy. This chapter describes how to set up RealPlayer to contact RealProxy.

Overview

Most clients, such as RealPlayer, contain an option to contact a proxy rather than sending requests directly to RealServers. In the client software, the user types the IP address (or host name) and port number of the proxy software to contact.

If you choose to connect clients to your RealProxy this way, you must either set up your users' client software yourself or send instructions to the users on how to set up the software themselves.

Configuring RealPlayers to Contact RealProxy

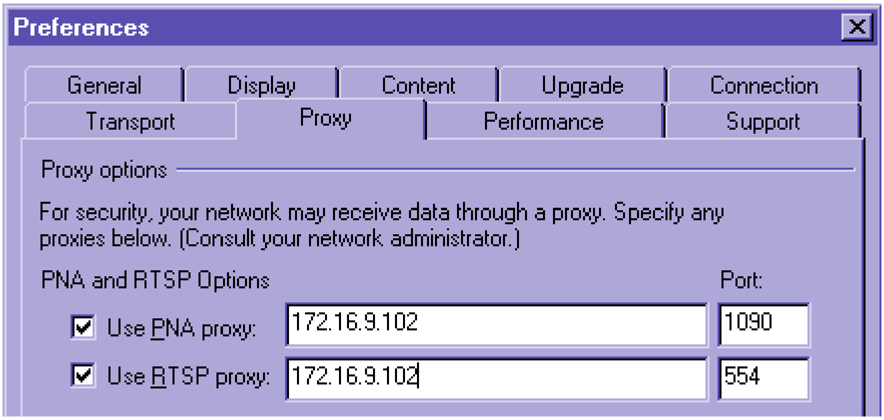
If you choose to configure RealPlayers to connect directly to RealProxy, use the instructions in this section.

➤ To configure RealPlayer:

1. In RealPlayer, select **View>Preferences**.
2. Select the **Proxy** tab.
3. Select the **Use PNA Proxy** box.
4. In the box next to it, type the IP address or host name of the RealProxy computer.
5. In the **Port** box, type the number of the RealProxy port number to which this client should send its PNA requests (usually `1090`). The number you type here must match the number in the **PNA Port** box on the Ports page in RealSystem Administrator.

6. Select the **Use RTSP proxy** box.
7. In the box next to it, type the IP address or host name of the RealProxy computer.
8. In the **Port** box, type the number of the RealProxy port number to which this client should send its RTSP requests (usually 554). The number you type here must match the number in the **RTSP Port** box on the Ports page in RealSystem Administrator.
9. Click **OK**.

RealPlayer Version 8.0 Proxy Tab



Proxy options

For security, your network may receive data through a proxy. Specify any proxies below. (Consult your network administrator.)

PNA and RTSP Options

		Port:
☑ Use PNA proxy:	172.16.9.102	1090
☑ Use RTSP proxy:	172.16.9.102	554

Chapter 6

ADVANCED FEATURES

This chapter covers features which are specific to the operating system, as well as reserving IP addresses for RealProxy's use, and running RealProxy on the same system as a Web server.

Reserving IP Addresses for RealProxy's Use

When RealProxy starts, it uses the primary IP address assigned to the machine's host name to listen for incoming requests. You can configure RealProxy to always listen on specific IP addresses by setting up the IP Binding list. Within this list, you cite individual addresses to use, or you use a special address to use all the IP addresses available on the RealProxy machine.

Note

The IP Binding list does not affect the address used for outgoing connections; those are determined by the operating system.

The recommended method is to capture all addresses for RealProxy's use by specifying the special IP address of `0.0.0.0`. If you specify this address, RealProxy automatically binds to all addresses and to the loopback address (`127.0.0.1`).

Or, if you only want to reserve certain addresses, put those addresses on the list instead. If you do bind to a specific address or addresses, you must also add the loopback address.

Warning

Use either `0.0.0.0` or a specific address (and loopback), but not both. If you use both, RealProxy will not start.

If you leave this feature blank, RealProxy binds to the primary host IP address and the loopback address. It does not bind to any other addresses.

Note

If a firewall is in use, you may need to configure it to allow traffic to pass on the addresses you added to the IP Binding list. See "Working with Multiple IP Addresses" for information.

➤ To bind to all IP addresses:

1. In RealSystem Administrator, click **General Setup**. Click **IP Binding**.
2. Click the **Add New** button.

   The address `0.0.0.0` appears in the Edit IP Address box.
3. Click **Edit**.
4. Click **Apply**.

Note

Remember, if you use `0.0.0.0`, there should be no other addresses on the list.

➤ To use specific IP addresses:

1. In RealSystem Administrator, click **General Setup**. Click **IP Binding**.
2. Click the **Add New** button.

   The address `0.0.0.0` appears in the Edit IP Address box.
3. In the **Edit IP Address** box, type the IP address that you want RealProxy to use.

Warning

Type the address carefully. If you type an IP address that does not exist on this computer, RealProxy will not be able to restart or to start. Should this happen, refer to "I can't start RealProxy at all." in Chapter 15, "Troubleshooting RealProxy".

4. Click **Edit**.
5. Repeat Step 2 through Step 3 for each address on this machine that you want RealProxy to use.
6. Click the **Add New** button.
7. In the **Edit IP Address** box, type the loopback address of `127.0.0.1`.

8. Click **Edit**.
9. Click **Apply**.

Running Web Servers and RealProxy on the Same System

If you install RealProxy on the same system as your Web server, you may need to complete additional steps. Most Web servers use port 80 for HTTP requests. At installation, RealProxy's default HTTP Port is 8080, but if you configure RealProxy to use port 80 (the same port as the Web server), problems may ensue. You may have to perform the following steps:

- Choose a different port for RealProxy to use for HTTP requests and change links that point to HTTP pages
- Reserve an IP address for RealProxy

Change the HTTP Port Value

Because RealProxy can serve requests for HTML pages sent via HTTP (such as RealSystem Administrator), if RealProxy is on the same system as a Web server, requests that begin with `http://` may be misdirected. When a user clicks a link that begins with `http://` and does not contain a port number, the client supplies a port number—80. When the Web server and RealProxy are on the same machine, the Web server will attempt to serve the file. If the link points to what's meant to be a RealSystem presentation, the Web server will not find the file and will display the error message "File not found."

To prevent this problem from occurring, make sure the HTTP Port value is not the same as the port number your Web server is using. The default value is `8080`. Most Web servers use port 80. Be sure that you include the port number in the URL.

Set IP Binding List

You may need to reserve at least one IP address for RealProxy's use, and instruct your Web server not to use that address. See "Reserving IP Addresses for RealProxy's Use".

Administering Both RealProxy and RealServer

If you are the administrator of both RealProxy and RealServer (for example, if you administer a corporate Web presence for both internal (RealProxy) and external (RealServer) use, or if you are an ISP host and you offer RealServer streaming services to your clients), here are some things to keep in mind:

- **Configuration file**—the structure of the configuration file is the same; only certain sections are unique to RealProxy.
- **Access log**—RealProxy's access log uses the same structure as RealServer, with additional information appended to the end of each record.
- **Pull splitting—**RealProxy's pull splitting method is nearly identical to the RealServer method of pull splitting, but RealProxy does not need to include the transmitter RealServer in the URL.
- **Multicast**—RealProxy has only one method of multicast, which is the same as RealServer's back-channel multicast. However, RealProxy can only multicast those incoming streams which are enabled for pull splitting on the transmitter RealServer.
- **Authentication—**Like RealServer, RealProxy authenticates users who access RealSystem Administrator. Unlike RealServer, however, RealProxy does not perform authentication on a per-clip basis. Instead, it allows or denies Player access to specific RealServers, by looking at the host name or address of the origin RealServer.

Features Specific to the Operating System

While RealProxy functions nearly identically on both Windows NT and UNIX platforms, there are a few differences that allow you to take advantage of unique characteristics of each operating system.

Windows NT

This section describes features unique to RealProxy running on a Windows NT system.

Windows NT Service

When you install RealProxy, you have the option to install it as a service. You can also configure this later. Several instances of RealProxy can be run from the same machine, with different configuration files.

Additional Information

See "Setting Up RealProxy as a Service".

UNIX

This section describes features unique to RealProxy running on a UNIX system.

User and Group Variables

The User setting indicates the user name under which RealProxy runs. The user name must exist on the computer on which RealProxy is running; otherwise, RealProxy will not start.

If you do not specify a user name when installing RealProxy, the user name defaults to the user name of the user who first logs in and starts RealProxy; this is accomplished with the default value of `%-1`.

The Group variable gives the group name under which RealProxy runs. The group name must already exist on the computer on which RealServer is running; otherwise, RealProxy will not start.

If you do not specify a group name, this variable defaults to the group name of the user who first starts RealProxy.

> **Note**
>
> Be sure that the user or group name you assign has write permissions for the `Logs` and `Secure` directories.

➤ To change the group or user names:

1. In RealSystem Administrator, click **General Setup**. Click **User/Group Name**.
2. Type the correct user name or ID number in the **User Name or ID** box. The default is `%-1`, which means RealProxy uses the user name of the user who logged in and started RealProxy.
3. Type the correct user name or i.d. number in the **Group Name or ID** box. The default is `%-1`, which means RealProxy uses the group name of the user who logged in and started RealProxy.
4. Click **Apply**.

Process ID (PID)

RealProxy creates a text file that stores the current value of the process ID of the main RealProxy file, `rmserver`. The file is stored in the directory indicated by the `PIDPath` variable (which you can see by opening the RealProxy configuration file), and is named `rmserver.pid` at installation. If `PIDPath` is omitted from the configuration file, RealProxy stores the information in the directory specified by the `LogPath` variable.

SIGHUP

Some changes that you make to RealProxy require that it re-read the changes while still running. Other changes require that RealProxy be restarted. If you use RealSystem Administrator to change settings, it will either force RealProxy to re-read the configuration file while RealProxy is still running (thus preserving all connections), or it will display a message instructing you to restart the Server at your convenience. The new settings will take effect once you restart RealProxy.

If you make changes to the configuration file manually, you will need to instruct RealProxy to re-read the configuration file. This is possible for RealProxy running on a UNIX platform with the **SIGHUP** command. Use the following command at a command prompt:

```
kill -HUP processID
```

where *processID* is the RealProxy process number, as shown in the `rmserver.pid` file.

Processor Count

On systems with multiple CPU processors, the `ProcessorCount` variable should be set to the number of processors available to RealProxy. If this variable is not present, RealProxy will use its automatic processor test, but the test may not be accurate if the system is busy doing other things when the test is performed.

You must manually configure this variable by editing the configuration file. The setting is:

```
<Var ProcessorCount="0"/>
```

The default value of `0` means that RealProxy will use its test to determine the number of processors available. If you have more than one processor on your system, you should change this variable.

FIREWALLS AND REALPROXY

Firewalls can inadvertently or deliberately block streaming media presentations, so familiarity with your network's firewalls will help you use RealProxy successfully. This chapter will help you configure your firewall for use with RealProxy.

Overview

A firewall is a software program or device that monitors, and sometimes controls, all transmissions between an organization's internal network and the Internet. Whether the network consists of a company's local area networks, wide area networks, and the Internet, or an Internet Service Provider, a firewall is typically deployed to prevent inappropriate access to the files, data, or machines of its customers. The firewall's role is to ensure that all communication, in both directions, conforms to the organization's security policies.

Often, firewalls permit one-way outbound access to the Internet. Because RealProxy needs to establish two-way communication with both clients and transmitter RealServers, firewalls can be problematic if they interfere with either of these necessary connections.

Who Should Read This Chapter

The next sections discuss the different possible firewall arrangements and illustrate how RealProxy works with them. This information will be of interest to anyone who wants to know:

- where to place RealProxy in relation to a network firewall
- why a firewall that allows RTSP and PNA traffic provides the best user experience
- why some clients are unable to receive clips, or receive them at poor bit rates

More information on firewalls is available from the RealNetworks Web site at **http://service.real.com/firewall**.

For information on configuring a specific firewall product, consult the firewall software's documentation.

Highlights of This Chapter

If a Server is behind a firewall, it can only stream content to other users behind the firewall. It cannot stream over the Internet to users on the other side of the firewall.

Additional Information
Read "How Firewalls Affect RealProxy".

For a Server that is streaming or broadcasting over the Internet, the best location is in the perimeter network, sometimes known as the de-militarized zone (DMZ).

Additional Information
See "Locating RealProxy Near the Firewall".

The firewall that provides the best user experience is one that allows RTSP and PNA application-layer traffic, and that allows use of the UDP transport protocol.

Additional Information
Refer to "Summary of Firewall Types".

How Firewalls Affect RealProxy

If a firewall separates any of the RealSystem G2 component software packages that communicate with each other–such as clients, RealProxy, and RealServer– the delivery of data may not occur at an optimal rate, or it may not occur at all.

For example:

- Firewalls configured to only allow TCP traffic may cause the user to see frequent buffering of clips.
- User experience of the presentation is compromised; greater latency and startup times affect the time needed to view the clip, and delivery of the clip requires more total bandwidth.

- If there is a firewall between RealProxy and a transmitter RealServer, RealProxy may not be able to send receive data via pull splitting.

There are three possible locations of firewalls in relation to RealProxy:

- between RealPlayer and RealProxy
- between RealProxy and RealServer
- in both locations

The effect of the firewall depends on the location of the firewall. They are described in the following sections.

Firewall Between RealPlayer and RealProxy

Ideally, the firewall should allow UDP and TCP traffic to travel from RealProxy to RealPlayer. At a minimum, it must permit TCP connections between the two products. Otherwise, RealPlayer will not receive any streaming media at all.

RealNetworks recommends that RealProxy be deployed on the same side of the network firewall as the clients.

Firewall Between RealProxy and RealServer

The firewall must permit RealProxy to make outbound TCP connections to at least ports 554 and 7070 so that RealProxy may connect to upstream RealServers.

Other transports and ports are required for specific RealProxy features:

- **Passthrough mode**—the firewall must permit UDP traffic to be sent to RealProxy through the firewall. Failure to do so will force RealProxy to receive passthrough streams via TCP, which increases opportunities for lost packets over congested network segments, thus causing client rebuffering or undesired start-up latency.

  Passthrough mode requires that the firewall allow inbound traffic to ports 6970 through 32000.

- **Pull splitting mode**—the firewall must allow UDP traffic to be sent to RealProxy through the firewall. By default, RealProxy expects to receive transmitter streams using the UDP transport. If UDP traffic is prohibited to the RealProxy on its splitter port, the **Protocol** option on the Pull Splitter page (`SplitterProtocol` variable in the configuration file) must be set to use TCP. Transmitter streams arriving at the RealProxy via TCP may result in client rebuffering or greater start-up latency upon client connection.

The firewall must allow inbound traffic to port 3030 for pull splitting to work.

- **Caching mode**—the firewall must enable RealProxy to make outbound TCP connections to RealServers on the cache transfer ports of the RealServer. Without connection to these ports, RealProxy cannot cache on-demand content, and will use passthrough mode instead.

  Caching requires that the firewall allow outbound connections on ports 7878 and 7802.

Firewalls and Their Interaction with RealProxy Features

This section explains how firewalls affect certain RealProxy features, and what changes you may need to make in RealProxy for it to work with your firewall. Those features which are unaffected by firewalls are not described.

Firewall Between the Client and RealProxy

RealProxy features affected by a firewall that separates RealProxy and clients are:

- Connecting to presentations
- Access Control
- Logging
- Multicasting

Connecting to Presentations

Issues that clients may have in connecting to presentations are described in "Communicating with Clients Behind Firewalls".

Access Control, Logging and Firewalls

When a firewall exists between a client and RealProxy, the IP address that appears in the access log's *client_IP_address* field may not be the true client address, and you might not get an accurate idea of exactly which clients are viewing material streamed by your RealProxy. See the "Address Shown in Access Log" table for a list of which firewalls replace the client's or Proxy's address with their own.

Multicasting and Firewalls

If a multicast is occurring through a firewall, the firewall must be specially configured to allow multicast traffic. Consult your firewall documentation for information on enabling multicast traffic.

Firewall Between RealProxy and RealServer

RealProxy features affected by a firewall that separates RealProxy and a transmitter RealServer are:

- **Pull splitting**—To allow pull splitting, the firewall must allow traffic on the pull splitting ports.
- **Caching**—As with pull splitting, a certain set of ports must be accessible.
- **Authentication**—Authentication information is handled over the control channel. If a firewall prevents the control channel connection, RealServer cannot authenticate the request and therefore will not deliver it. The control channel is described in the next section.

Refer to the “Ports Used by RealProxy” table for specific information.

Protocols Used by RealSystem

RealSystem applications uses two connections, known as “channels,” to communicate: one for sending and receiving instructions, and one for actual data. The first channel is known as the “control channel,” since it is over this line that RealServer requests and receives passwords, and the client sends instructions such as play, pause, and stop. Media is actually streamed over a separate “data channel”.

Both RealServer and RealProxy use two sets of protocols in transmitting data:

- **Control channel**—uses application-layer protocols RTSP and PNA
- **Data channel**—uses transport protocols TCP and UDP

Application-Layer Protocols

RealProxy and RealServer use two application-layer protocols to communicate with clients: RTSP (Real Time Streaming Protocol) and PNA (Progressive Networks Audio). These protocols establish a two-way TCP connection to send commands from the client such as “start” and “pause,” and from RealServer to clients for information such as the clips’ titles.

- RTSP is an open standard client/server protocol designed specifically for serving multimedia presentations. It is useful for large-scale broadcasting. Only RTSP can deliver SureStream™ files, which use multiple bandwidth encoding, and automatically choose the best available presentation for the user's available bandwidth.
- PNA is the proprietary client/server protocol designed and used in previous software versions. The ability to serve via PNA is supported in RealServer for compatibility with older versions of RealPlayer.

Control and Data Channel Protocols

Control Channel Protocol	Data Channel Protocol
RTSP	TCP and UDP, or TCP only
PNA	TCP and UDP, or TCP only

As we will see later in this chapter, the single TCP protocol may be used if a firewall does not permit UDP connections that originated outside the firewall.

Transport Protocols

The quality of the stream received by a client is related to the transport protocol in use.

- For the control connection, RealSystem uses the two-way Transmission Control Protocol (TCP) protocol.

  The TCP protocol guarantees delivery of packets, which is important for control information and error-checking. It has built-in congestion control, but it is slow to respond to changing network conditions. Because TCP is a two-way connection protocol, the client and the Server can communicate about passwords; the user can press pause or fast-forward and the information is sent over the TCP connection. However, verification that each set of instructions reached its intended destination consumes some overhead.

  The characteristics of TCP which make it suitable for control information also make it less appropriate for continuous data delivery. The overhead used in TCP is not optimized for the delivery of streaming media.
- For the data connection, RealProxy and RealServer use the one-way User Datagram Protocol (UDP) protocol.

UDP packets are sent in one direction only. Because the transport does not perform error checking, it can deliver the packets faster than TCP does.

RealProxy and RealServer use TCP to send presentations to the media cache.

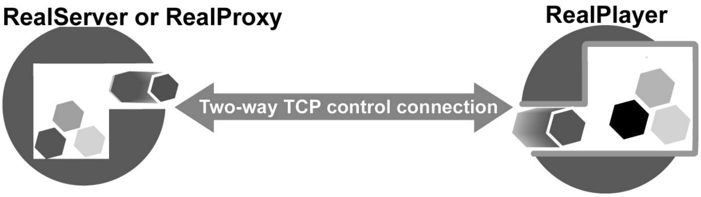
Communicating with Software Behind Firewalls

Information in this section applies to administrators of RealProxy who are interested in the nature of the connection between RealProxy and other RealSystem software.

Communicating with Clients Behind Firewalls

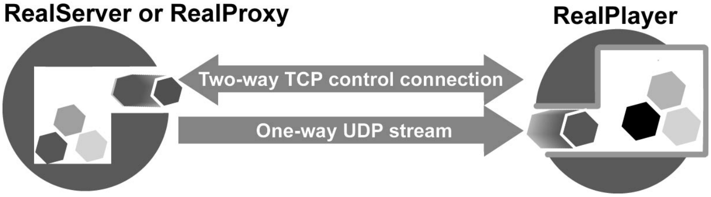
When no firewall exists between RealProxy and the client (such as when they are both in the same internal network), the client software first tries to establish a two-way TCP control connection to RealProxy. The Proxy uses this connection initially as a means of sending information to the client about the requested media, such as the name, length, and copyright of the clip. The client uses the connection to send commands to RealProxy when features such as the Play and Stop buttons are activated.

Initial Connection Between RealServer and Client, or Between RealProxy and Client



After the initial connection is established, RealProxy then establishes a data channel back to the client. The actual media is sent along this channel, which uses UDP.

Data Channel Between RealServer and Client, or Between RealProxy and Client



How Clients Communicate with a RealProxy from Behind a Firewall

This section explains the logic used within the client software as it tries to contact your RealProxy.

To optimize playback quality, clients are designed to automatically try different methods of connecting to RealProxy to work through common firewall configurations.

The list below shows how the client software determines what protocol it will ask RealProxy to use in sending the streamed media over the data channel.

1. The client attempts to open a control connection, using TCP. It uses port 554 for the RTSP protocol, or port 7070 for the PNA protocol.
   - If the firewall does not allow TCP on 554 (or port 7070), the request is denied and the user sees an error message.
   - If the firewall permits the TCP connection, the client goes to Step 2.
2. Now that a TCP control connection has been established, the client attempts to set up the data channel.

   If the request is for on-demand content, the client tries these methods:

   a. First, it tries UDP, in the range of port 6970 through 32000. (Earlier versions of RealPlayer used a smaller range. Consult the "Ports Used by RealPlayer" table.)

   b. If UDP is not allowed, it requests that the data be sent via TCP on the established control channel.

   If the request is for live content, the client tries three connection methods:

   a. First, it tries to use multicast. This is a specialized option not available on many networks. Multicast uses the UDP transport protocol and may use either the RTSP or PNA application-level protocol. Firewalls must be specially configured to allow multicast traffic.

   b. If multicast is not available, the client requests that the material be sent via UDP on ports 6970 through 6999.

   c. If UDP cannot pass through the firewall, the client requests delivery via TCP on the established control channel.

Users can configure RealPlayer to always use a particular protocol and port as directed by their firewall administrator.

Additional Information

Refer to *RealPlayer Plus G2 Manual* for instructions on setting preferences in the client. See **http://service.real.com/help/library/index.html**.

Allowing Pull Splitting to Work Through Firewalls

By default, RealProxy and RealServer use UDP to communicate in pull splitting mode. An option is available for them to use TCP instead.

➤ To change the protocol for splitter-to-Server communication:

1. In RealSystem Administrator, click **Splitting**. Click **Pull Splitter**.
2. In the **Protocol** box, select TCP.
3. Click **Apply**.

Working with Multiple IP Addresses

If your firewall expects to allows connections to transmitter RealServers only from certain IP addresses, make sure that it permits traffic on all the addresses used in the IP Bindings list.

When the machine on which RealProxy is running has multiple IP addresses (either multiple Network Interface Cards or virtualized addresses), and you use the IP Bindings feature to instruct RealProxy to use those addresses, RealProxy will make its outgoing connections using the operating system's routing table.

Consider the following addresses, which could be listed in the IP Bindings feature (described in "Reserving IP Addresses for RealProxy's Use"):

```
172.16.0.1
172.16.0.2
```

If a client connects to RealProxy on address `172.16.0.1`, RealProxy will forward the request to the transmitter RealServer using `172.16.0.1`. This same address will appear in the transmitter RealServer's access log. Another client that connects on `172.16.0.2` will have its request sent along using `172.16.0.2`. The IP address of `172.16.0.2` will appear in the transmitter RealServer's access log.

Firewall Configurations (For Firewall Administrators)

This section describes firewall types, the best way to configure your firewall to permit streaming media, and lists the port numbers used by RealProxy.

Firewall Types

Firewalls can be categorized into roughly six types. A particular firewall vendor may combine more than one type into a particular product. The type of firewall in use by your organization will affect the method that RealProxy uses to stream content to clients.

- Application-level proxy
- Transparent proxy
- Packet filter
- Stateful packet filtering
- SOCKS
- Network address translation

The address that appears in the access log of the transmitter RealProxy depends on the client's type of firewall.

A firewall monitors every type of transmission between client software and the Internet, but this discussion looks only at the firewalls' effects on streaming media.

Application-Level Proxy Firewall

Application-level firewalls first determine if a requested connection between a computer on the internal network and one on the outside is permitted. If the connection is authorized, the firewall mimics the requesting software and sets up the necessary communication links between the two computers. As an intermediary, the firewall can monitor the communication between the two networks and suppress any unauthorized activity.

Because an application-level firewall acts as an intermediary between RealPlayer and RealProxy (or between RealProxy and RealServer), the firewall itself must know how to handle the RealPlayer protocols (RTSP and PNA).

The user must configure the client software to contact a proxy or firewall machine. (In RealPlayer, this setting is located under **Options>Preferences> Proxy**.)

Transparent Proxy Firewall

A network administrator configures the firewall to intercept requests for streaming media.

Packet Filter Firewall

Rather than impersonating an application, network-level firewalls examine the packets of information sent at the transport level to determine whether a particular packet should be blocked. Each packet is either forwarded or blocked based on a set of rules defined by the firewall administrator.

A common configuration for network-level-filtering firewalls is to allow all connections initiated by machines inside the firewall, and to restrict or prohibit all connections made by machines outside the firewall. For most programs, this works well since they usually only establish a single outbound TCP connection.

However, RealPlayer and RealProxy (or RealProxy and RealServer) maintain two simultaneous connections: a TCP connection for sending commands and a UDP connection to stream the actual media according to the instructions received via TCP. The TCP connection initiated by the Player for controlling the connection will work through a packet filter firewall. Since network-level filters block UDP as a matter of course, the UDP stream sent by the RealServer or by RealProxy will be deflected off the firewall and never reach the Player that made the request.

Stateful Packet Filtering Firewall

A stateful packet filtering firewall monitors the communication between the client and the Internet to ensure that inbound packets are being sent at the request of a client inside the firewall. Similar to packet filters, it may include additional options that allow more sophisticated actions to be taken with individual packets.

These firewalls should be configured to permit RTSP and PNA traffic.

Network Address Translation Firewall

A network address translation firewall converts the client’s internal address to an external address before it forwards the client’s requests to RealServer. Once it receives a request, RealServer will send its UDP packets directly to the firewall, rather than to the client, and the firewall may not know which client requested the packets. Network address translation is often implemented as part of packet filtering firewalls or stateful packet filtering firewalls.

SOCKS Firewall

Only software with built-in SOCKS support, that must additionally be configured by the user, can send data through a SOCKS firewall; RealPlayer does not include SOCKS support.

In some cases, a user can install a Winsock.dll that supports SOCKS, and configure it to point to the SOCKS firewall.

Summary of Firewall Types

The table below summarizes the six most common firewall types and any special configuration information.

Streaming Media Over the Firewall Types

	Client configuration required?	IP address seen by the client	IP address seen by the Server (in access log)	Valid inside addresses required?	RTSP support required to get UDP?	RTSP support required to get TCP?
Application-level proxy	Yes	Firewall's address	Firewall's address	No *	Yes	Yes
Transparent proxy	No	Server	Firewall	No*	Yes	No**
Packet filter	No	Server	Client	Yes	No	No
Stateful packet filtering	No	Server	Client	Yes	No	No
Address translation	No	Server	Firewall	No*	Yes	No
SOCKS	Yes	Firewall	Firewall	No*	No***	No

* Usually requires compliance with RFC 1597 Address Allocation for Private Internets (http://www.ietf.org/rfc/rfc1597.txt)

** May require special configuration

***Requires SOCKS version 5.0

Some firewalls are actually a mix of the firewall types described in the preceding section.

Depending on the type of firewall and its location, the client address shown in the access log may not reflect the true address of the client. The table below lists the address that will appear in the access log as the requesting client's address.

Address Shown in Access Log

	Firewall between client and RealProxy	Firewall between RealProxy and RealServer	
Firewall type	Address shown in RealProxy's access log	Address shown in RealProxy's access log	Address shown in RealServer's access log
Application-level proxy	Firewall's address	Client	Firewall's address
Transparent proxy	Firewall	Client	Firewall
Packet filter	Client	Client	RealProxy
Stateful packet filtering	Client	Client	RealProxy
SOCKS	Firewall	Client	Firewall
Address translation	Firewall	Client	Firewall

Best Firewall Arrangements

The firewall that provides the best experience for RealSystem software users is one that allows streaming media, by enabling TCP and UDP traffic. See the "Ports Used by RealProxy" table for a complete list of ports that need to be open.

- Several firewall vendors already include this type of streaming media support. View the RealNetworks firewall page at **http://service.real.com/firewall** to find a vendor.
- You can modify your existing firewall with the help of the free RealNetworks Firewall Administrator's Proxy kit.

The next best option is a firewall that allows a TCP control channel and a TCP data channel. Your firewall administrator can easily make this change to the firewall. However, the quality of the connections will not be as good with this configuration.

Locating RealProxy Near the Firewall

A realistic deployment of RealProxy within or near a secure network is to place it inside a network firewall or in a secure perimeter network (sometimes known as a De-Militarized Zone, or DMZ). In such a deployment, it is typical that clients are not allowed to access the public internet or other non-local networks directly; instead, clients send their requests to RealProxy, which is enabled to make and receive Internet connections outside the secure network. In this arrangement, only RealProxy is exposed to network traffic beyond the confines of the secure firewall.

The firewall must allow the following types of connections:

- All RealPlayers residing within the secure network need to connect to RealProxy using TCP.
- RealProxy needs to be able to send both TCP and UDP traffic to its clients.
- If RealProxy is contacting transmitter RealServers that are outside the secure network, the firewall must allow it to make outbound TCP connections on several ports. Additionally, UDP traffic will need to be received by the RealProxy from those remote RealServers.

Refer to the next section, "Ports Used by RealSystem", for specific information on the ports that are needed.

Ports Used by RealSystem

Information in these tables will help you decide which ports to open on your firewall. For more detailed information, especially if you do not want to explicitly open all the ports listed, refer to the documentation on the RealNetworks Web site, at **http://service.real.com/firewall**.

These tables do not cover use of port numbers in multicasting.

Port Numbers Used by RealProxy

Ports used by RealProxy are shown below.

Ports Used by RealProxy

Listen On or Send To	Port Number	Protocol	Purpose
Communicating with RealPlayer, Communicating with a Child RealProxy			
Listen on	554	TCP	RTSP proxy requests
Listen on	1090	TCP	PNA proxy requests
Send to	6970-6999	UDP	Data channel (port numbers are not configurable)
Communicating with RealServer			
Send to	554	TCP	Control channel for RTSP requests to RealServer
Send to, Listen on	3030	TCP or UDP	Data and control channel for pull splitting via TCP. Control channel for pull splitting via UDP.
Listen on	6970 - 32000	UDP	Data channel for inbound UDP.
Send to	7070	TCP	Control channel for PNA requests to RealServer
Send to	7878	TCP	Cache requests to RealServer
Communicating with RealSystem Administrator			
Send to	9090	TCP	Java Monitor traffic
Listen on	Admin Port	TCP	RealSystem Administrator
Communicating with a Parent RealProxy			
Send to	554	TCP	Control channel for RTSP requests to parent RealProxy
Send to	554	TCP or UDP	Data and control channel for pull splitting
Send to	1090	TCP	Control channel for PNA requests to RealProxy
Send to	7878	TCP	Cache requests to RealProxy
Listen on	6970-32000	UDP	Data channel

Port Numbers Used by RealPlayer

In addition to the settings shown below, RealPlayer inherits proxy settings (if they exist) from the default browser. If they change in the browser, the changes are reflected in RealPlayer. Users can turn off this feature from the RealPlayer Preferences menu.

The ports used in sending requests to RealProxy (usually 1090 and 554) may be different if the client is configured to contact RealProxy through a different method. Refer to Chapter 7, “Firewalls and RealProxy” for information.

Ports Used by RealPlayer

Listen On or Send To	Port Number	Protocol	Purpose
RealPlayer versions 6.0 and later, communicating with RealServer or RealProxy			
Send to	1090	TCP	Control and data channel, used in sending requests to RealProxy.
Send to	554	TCP	
Send to, Listen on	6970 - 32000	UDP	Data channel
RealPlayer versions 3.0 through 5.0, communicating with RealServer or RealProxy			
Listen on	6970 - 6999	UDP	Data channel (not configurable)

Port Numbers Used by RealServer

Normally, the client software chooses UDP for the data channel, and indicates a port number between 6970 and 6999 on which it will receive the data. RealServer receives the request on port 554 (if requested via RTSP) or port 7070 (if requested via PNA), and directs the data to the port number specified by the client.

If the client software chooses TCP for the data channel, RealServer uses the same port number for both the control channel and the data channel. If the clip was requested using RTSP, both channels will use port 554. If the clip was requested using PNA, both channels will use port 7070.

This table shows the typical values used by RealServer in conjunction with RealProxy.

Ports Used by RealServer

Listen On or Send To	Port Number	Protocol	Purpose
Communicating with RealPlayer			
Listen on	554	TCP	Control channel for RTSP requests (data channel also, if TCP was requested)
Listen on	7070	TCP	Control channel for PNA requests (data channel also, if TCP was requested)
Listen on	8080	TCP	HTTP requests
Send to, Listen on	6970-6999	UDP	Data channel (port numbers are not configurable)
Communicating with RealProxy			
Listen on	3030	TCP or UDP	Data channel for pull splitting requests
Send to	6970-32000	UDP	Data channel (port numbers are not configurable)
Listen on	7802	TCP	RealProxy requests
Listen on	7878	TCP	RealProxy requests

Chapter 8

MANAGING BANDWIDTH

RealProxy uses several methods for managing bandwidth. Whether you implement just one method, or you use several in conjunction, you have the ability to control the amount of streaming media traffic on your network.

Overview

When you install RealProxy, the values for each of these settings is configured to use the maximum available number.

Techniques for managing the bandwidth you use include:

- **Maximum Client Connections**—limits the number of clients that can connect at one time.
- **Maximum Proxy Bandwidth**—restricts the bandwidth in use between RealProxy and clients.
- **Maximum Gateway Bandwidth**—restricts the bandwidth in use between RealProxy and RealServers.

The default value for each technique is 0, which means RealProxy will use the maximum amount permitted by your license.

If you establish values for all these features, RealProxy will limit access when the lower threshold is reached. If a client tries to make a request after a limit has been reached, the client receives an error message.

In addition, you can require that the only certain client versions can connect to your RealProxy.

For information on restricting which clients can connect to RealProxy based on their IP addresses, see Chapter 9, “Limiting Access to RealProxy”.

Maximum Client Connections

By using the **Maximum Client Connections** setting, you can limit the number of clients who connect simultaneously. Once this limit is reached, clients that attempt to connect receive an error message, and will not be able to connect until other clients disconnect.

➤ To limit access by limiting connections:

1. In RealSystem Administrator, click **General Setup**. Click **Bandwidth Management**.
2. In the **Maximum Client Connections** box, type the number of client connections you want to allow simultaneously.

   This number can be from `1` to `32767`, as long as it is less than or equal to the number of streams permitted by your license. If it is `0` or blank, RealProxy uses the number of streams specified by your license. The default value is `0`.
3. Click **Apply**.

Maximum Proxy Bandwidth

The **Maximum Proxy Bandwidth** setting limits the amount of bandwidth RealProxy consumes, in kilobits per second (Kbps).

For example, if you set this number to 100, two clients each play 50 Kbps clips, or one can play a 40 Kbps clip and another can play a 60 Kbps clip.

If the first client requested an 80 Kbps clip, a second client can also receive an 80 Kbps clip, even though RealProxy is now using more than 100 Kbps. However, no new clients will be permitted to connect, as the maximum bandwidth use has been reached.

➤ To limit client bandwidth:

1. In RealSystem Administrator, click **General Setup**. Click **Bandwidth Management**.
2. In the **Maximum Proxy Bandwidth** box, type the maximum number of kilobits per second (Kbps) that should be in use at once.

   For example, to limit the bandwidth to one megabyte, specify maximum bandwidth usage by setting **Maximum Proxy Bandwidth** to `1024`.
3. When you have finished making changes, click **Apply**.

Maximum Gateway Bandwidth

You may want to limit the amount of bandwidth RealProxy acquires, whether from another RealProxy, RealServer, or the Internet.

Limiting gateway bandwidth limits the following RealProxy functions:

- passthrough data connections
- pull splitter data connections
- initial cache requests

The number in Maximum Gateway Bandwidth is given in kilobits per second (Kbps). RealProxy will make no new upstream connections once the gateway threshold has been crossed.

For example, if you set this to 2048, and RealProxy made one connection that used 1024 Kbps, it can still make a connection of 1600 Kbps (even though the total Kbps in use is now 2624), but no new connections can be made after that.

➤ To limit RealProxy-to-gateway bandwidth:

1. In RealSystem Administrator, click **General Setup**. Click **Bandwidth Management**.
2. In the **Maximum Gateway Bandwidth** box, type the maximum number of kilobits per second (Kbps) that RealProxy should use when it connects to its gateway.

   For example, to limit the bandwidth to two megabytes, specify maximum bandwidth usage by setting **Maximum Gateway Bandwidth** to `2048`.
3. When you have finished making changes, click **Apply**.

Limiting Access to Multicast Reception

By setting **Delivery Only** to `Yes` in the multicast list, you can require that clients within a certain range of IP addresses connect only in multicast mode. When this option is set to `Yes`, clients that are not able to connect in multicast mode receive an error message. If this option is `No`, clients that cannot connect in multicast mode can use unicast mode to receive the presentation.

This feature is described in Chapter 11, “Multicasting Live Streams”.

Chapter 9

LIMITING ACCESS TO REALPROXY

In this chapter, you'll learn how you can restrict access to certain clients based on their IP addresses.

Overview

You can block or permit access to specific RealProxy ports based on the IP address of the client and the port to which they are sending their requests. Clients whose IP addresses are configured with "deny" receive an error message indicating that the URL is not valid or that the connection has timed out.

For example, you can restrict which clients can send requests to your RealProxy by restricting access to the RTSP Proxy port (usually 554).

Additional Information

To learn how to give access to RealSystem Administrator based on user name, see "Restricting Access to RealSystem Administrator".

Information about each IP address or range of addresses you want to allow or restrict is stored in a rule. A rule is a set of instructions to RealProxy about the address range and behavior to allow. Rules are identified by numbers which you assign.

Each rule contains the following information:

- **Access Rule Number—**Identification number for this rule.
- **Access—**Whether the client will be allowed or denied access.
- **Client IP Address—**Client's address, or a range of addresses.
- **Client Netmask**—Client's netmask.
- **Server IP Address—**RealProxy's address.
- **Ports—**Port numbers to which access is specified.

When a client attempts to play a RealProxy presentation, RealProxy compares the client's address and the requested port to the addresses and ports listed in the rules.

Before using this feature, you must make decisions about the types of rules you will create. You can create as many rules as you like.

Creating Rules

There are two ways you can restrict access, and these determine how you set up the rules.

- **Specific Address Denial**—Deny a specific group of IP addresses and ports, and allow access to everyone else.
- **Specific Address Permission**—Allow a specific group of IP addresses and ports, and deny access to everyone else.

When you create a rule, you give it a number. RealProxy uses these numbers to sort the rules before it looks at a client's request. You do not have to create the rules in a certain order; RealProxy will perform the sorting automatically.

RealProxy compares the client's IP address and requested port to the sorted rules, beginning with the lowest-numbered rule. As soon as RealProxy finds a rule that matches the client's address, it allows or denies access, according to the rule's characteristics.

Tip

Rule numbers can be any length, but a number of more than one digit allows you to quickly add more rules later, without renumbering existing rules. Also, because RealProxy examines the rules in numeric order, you should make the lowest-numbered rules the most strict. Reserve high rule numbers for the most lenient rules. This is similar to the schema for firewall addresses.

The following table summarizes the denial/permission sets of rules, and suggests numbering schemes.

Suggested Rule Schemes

	Specific Address Denial	Specific Address Permission
Rule Set	Contents of Rules in Each Set	
Rule 0: Built-in rule. Do not edit this rule.	This rule permits access to RealProxy from an application running on the same computer.	
Rule 1: Built-in rule. Do not edit this rule.	This rule prevents other computers from accessing ports 6060 and 7070, which are reserved for RealProxy's use.	
Rule 2: Specific client addresses Suggested rule numbers: 2 - 49 Rule 2 is supplied, but you may edit it.	Clients **prevented** from accessing RealProxy. Client IP address: specific client addresses. **Access**: `Deny` **Ports**: use values for specific ports	Clients **permitted** to connect to RealProxy. Client IP address: specific client addresses. **Access**: `Allow` **Ports**: use values for specific ports
All other addresses Suggested rule numbers: 50 - 99	Clients **permitted** to use your RealProxy. **Client IP address**: `Any` **Access**: `Allow` **Ports**: use values for content ports	Clients **prevented** from using RealProxy. **Client IP address**: `Any` **Access**: `Deny` **Ports**: use values for specific ports This set of rules is optional.
Access to RealSystem Administrator Suggested rule number: 100	All clients not listed in either of the rules above. **Client IP address**: `Any` **Access**: `Allow` **Ports**: use value for *Admin Port*	All clients not listed in either of the rules above. **Client IP address**: `Any` **Access**: `Allow` **Ports**: use value for *Admin Port*

Setting Up IP Access Control

There are two steps to setting up access control rules, regardless of which method you chose in "Creating Rules":

1. Set up general rules which allow you to remain connected to RealSystem Administrator. You need only perform this set of steps once.
2. Create rules for specific IP addresses and port numbers.

Creating General Access Rules

The steps in this section create a rule that allows you to connect to RealSystem Administrator, regardless of the restrictions you create in other rules. Although it appears that you are allowing everyone to access RealSystem Administrator, the only people who will use it are other administrators who know the Admin Port number (chosen randomly at installation) and who have a user name and password specifically for RealSystem Administrator.

Warning

If you omit this initial step, you will not be able to connect to RealSystem Administrator when you restart RealProxy, regardless of whether you have username-and-password permission.

➤ To allow access to RealSystem Administrator:

1. In RealSystem Administrator, click **General Setup**. Click **Ports**.

   Make a note of the **Admin Port** number. (This is the same number as the port number shown in your browser URL.)
2. In RealSystem Administrator, click **Security**. Click **Access Control**.
3. In the Access Rules area, click **Add New**.

   A generic access rule number appears in the **Edit Rule Number** box.
4. In the **Edit Rule Number** box, type `100`.
5. Click **Edit**.
6. From the **Access** list, select `Allow`.
7. In the **Client IP Address** box, type `any`.
8. In the **Server IP Address** box, type `any`.
9. In the **Ports** box, type the Admin Port number you noted in Step 1.
10. Click **OK**.
11. Click **Apply**.

You will now be able to access RealSystem Administrator, no matter what rules you create in the next section.

Creating Specific Access Rules

Use the steps in this section to allow or deny access to specific IP addresses or address ranges.

Warning

Be sure to first follow the steps in "Creating General Access Rules", or you will not be able to access RealSystem Administrator after you restart RealProxy.

➤ To limit access according to IP number:

1. Determine the port numbers in use. You'll use these in Step 10. Click **General Setup>Ports**.

   Make a note of the values for **PNA Proxy Port** (usually `1090`) and **RTSP Proxy Port** (usually `554`).

2. In RealSystem Administrator, click **Security**. Click **Access Control**.
3. In the Access Rules area, click **Add New**.

   A generic rule number appears in the **Edit Rule Number** box.

4. In the **Edit Rule Number** box, type a number for the new access rule in the **Access Rule Number** box.
5. Click **Edit**.
6. Indicate whether permission is being granted or refused by selecting `Allow` or `Deny` from the **Access** list.
7. In the **Client IP Address** box, type the IP address of the client machine.

   Tip

   To refer to any IP address, type `Any` in the **Client IP Address** box, and leave the **Client Netmask** box blank.

8. Type a value in the **Client Netmask** box if you want to indicate a range of client addresses.
9. In the **Server IP Address** box, type the IP address of the client machine or network card.

   You can type a specific address, or use the word `Any` to refer to any IP address on the RealProxy machine.

If you type a specific IP address or host name, rather than the word `Any`, you must also add that address to the IP Binding list. See "Reserving IP Addresses for RealProxy's Use" for more information.

10. Finally, list the RealProxy port numbers to which you want to restrict access. In the **Ports** box, type the port numbers you noted in Step 1, separated by commas. For example, type `1090, 554`.
11. Click **Apply**.

Chapter 10

PROXY ROUTING

For networks that handle Internet-bound requests with strict rules, RealProxy can be configured to route requests for material delivered by certain RealServers through another RealProxy. This chapter explains how to set up proxy routing.

Overview

Proxy routing, sometimes known as chaining or parent/child, allows you to route RealProxy requests through other RealProxys.

The proxy routing feature instructs RealProxy to look at the address of the requested material, and to send it either to a specific RealProxy, or to send it directly to the RealServer that hosts the content.

The main RealProxy which handles requests bound for the Internet is called the parent RealProxy; the RealProxys located closest to the clients are called child RealProxys.

Typical uses for this feature include routing all requests for locally-served material directly to the RealServer, and forwarding all other requests through a gateway RealProxy.

Notes on Deploying This Feature

A parent RealProxy can also stream content to clients while simultaneously streaming data to a child RealProxy. While it is technically possible for a child RealProxy to also act as a parent RealProxy, it is not recommended.

Warning

This feature is designed specifically for enterprise scenarios in which subnet traffic is routed through proxy software. Proxy routing is not recommended for use in any other scenarios, as the increased latency and administrative overhead are appropriate only to controlled network situations.

Rules for Routing

Each child RealProxy directs its streams to other RealProxys by use of rules.

Rules are sorted in the order in which they appear in RealSystem Administrator. Therefore, it makes sense to put the rules which affect the most requests later in the list. Put the most specific rules first.

Use an asterisk (*) to indicate a wildcard section. There are some conditions for using the wildcard:

- You may use only one asterisk per rule. For example, `*.example.com` is a valid entry in the **Routing Table** box, but *.example.* is not. The following are all valid:

  `*` (forwards all requests to the RealProxy shown in the list)
  `*.com` (forwards all requests that end in .com)

  ```
  *.net
  *.example.com
  realproxy.*.com
  realproxy.example.*
  realproxy.department.example.*
  ```

- The asterisk cannot be used with a string. It can be used only within periods. Thus, `real*.example.com` is not valid.

Proxy Routing and RealProxy Features

This section describes how proxy routing works with three of RealProxy's features.

Passthrough

The passthrough feature under proxy routing works like this:

1. The client requests a stream through the child RealProxy. The child RealProxy proxies the request and sends it to the parent RealProxy outside the subnet. The parent RealProxy makes the request of the transmitter RealServer. The transmitter sends the data to the parent RealProxy.
2. The child RealProxy streams the request to the client.

The parent RealProxy maintains the control connection to the transmitter RealServer; the child RealProxy doesn't contact the transmitter RealServer directly.

Caching

With caching, the parent RealProxy always forwards the cache data to the child RealProxy; it does not store cache data itself. If a client requests the same data directly from the parent RealProxy, that RealProxy must still contact the transmitter RealServer before filling its cache, even though it has sent the same data to the child RealProxy. This prevents the parent RealProxy cache from filling with data it hasn't requested.

Caching under proxy routing works like this:

1. The client requests an on-demand stream, via the child RealProxy. The child RealProxy proxies the request and sends it to the parent RealProxy outside the subnet. The parent RealProxy makes the request of the transmitter RealServer. The transmitter sends the data to the parent RealProxy.
2. The child RealProxy caches the data and streams the request to the client.

Notice that the parent RealProxy does not fill its cache with the data.

Pull Splitting

The following steps show proxy routing with the pull splitting feature:

1. The client requests a stream, via the child RealProxy. The child RealProxy proxies the request and sends it to the parent RealProxy outside the subnet. The parent RealProxy makes the request of the transmitter RealServer. The transmitter sends the data to the parent RealProxy.
2. The child RealProxy streams the data to the client.
3. The second client to request the same material from the child RealProxy receives a split stream.

Notice that the splitting happens at the child level. A control connection is maintained with the transmitter, by way of the parent RealProxy. Splitting does not happen at the parent RealProxy; if a client connects to the parent RealProxy and requests the same stream, the parent RealProxy must proxy the request to the transmitter in the usual manner and splits that stream.

Customizing Proxy Routing Settings

When adjusting the proxy routing settings, you make changes to the child RealProxy only. You do not need to make any changes to the parent RealProxy.

➤ To set up proxy routing:

1. In RealSystem Administrator, click **General Setup**. Click **Proxy Routing**.
2. In the **Routing Table** area, click **Add New**.

   A generic rule name appears.
3. In the **Edit Rule** box, type the rule information you want this child RealProxy to use.
4. Click **Edit**.
5. If this rule points involves a parent RealProxy (rather than simply allowing all requests that fit the rule to pass directly to a transmitter RealServer), use the following steps:

   a. From the **Use Parent Proxy** list, select `Yes`.

   b. In the **Parent Name** box, type the host name or the IP address of the parent RealProxy where the client's request should be directed.

   c. In the **RTSP Parent Port** box, type the port number of the parent RealProxy to which requests for RTSP should be directed.

      Match the parent RealProxy's value for **RTSP Proxy Port** (usually `554`).

   d. In the **PNA Parent Port** box, type the port number of the parent RealProxy to which requests for PNA should be directed.

      Match the parent RealProxy's value for **PNA Proxy Port**, usually `7070`.

   e. In the **Parent Cache Port** box, type the port number of the parent RealProxy to which cache requests should be directed.

      Match the parent RealProxy's value for **Cache Port**, usually `7878`.
6. Repeat Step 2 through Step 5 for each rule that you will be adding.
7. If you didn't add the rules in the order described in "Rules for Routing", reorder them using the up and down buttons located next to the **Routing Table** box.
8. Click **Apply**.

Chapter 11

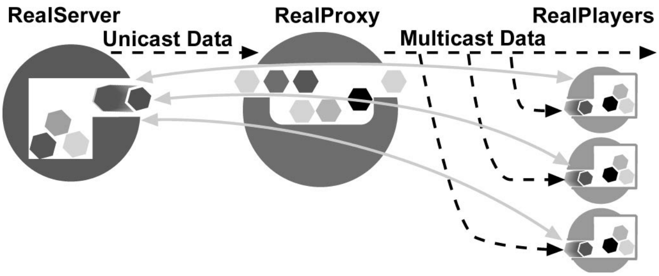
MULTICASTING LIVE STREAMS

Multicasting helps you conserve bandwidth. It requires a specially configured network. In this chapter, you'll see how to set up RealProxy to multicast.

Overview

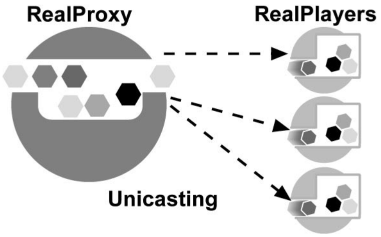
Multicasting is a way of sending a single live stream to multiple clients, rather than sending a stream to every single client.

Multicasting



In contrast, regular unicasting transmission sends a stream to each client that requests it.

Unicasting



To take advantage of multicasting, both RealProxy and clients, as well as the routers between them, must be multicast-enabled. For this reason, multicasting is mostly used with intranets where routers can be configured for multicasts. Multicast delivery can be done over the Internet only where intermediary network devices have been multicast-enabled.

Multicast is automatically used (when available and configured) for pull split streams. It is not used with passthrough or cache mode.

Multicast Methods

This method of multicasting uses the RTSP protocol to send control information over a TCP channel. RealProxy maintains a control connection for each client. The data channel is multicast to all clients. RTSP multicast provides the following features:

- **Connection statistics**—RealProxy can receive client connection information.
- **SureStream**—these multiply-encoded files are supported.

Note

RTSP multicasting works only with RealSystem G2 clients.

Setting Up Multicasting

Before you set up multicasting, you need to do two things:

- Configure the network for multicasting.
- Select the addresses you'll use for your multicasts.

Setting Up the Network for Multicasting

Before setting up RealProxy, verify the following items with your network administrator:

- Routers in your network are multicast-enabled.
- The computer running RealProxy is correctly configured for multicast support.

In addition to network settings, clients must be configured to request multicast transmission of live material. Consult the client software's user guide for information on configuring the client.

As noted earlier, both RealProxy and clients, as well as the routers between them, must be multicast-enabled in order for you to distribute presentations using the multicast features. This section describes only what is required to enable RealProxy for multicast broadcasting.

Allocating Addresses and Port Numbers in RealProxy

There are two factors to take into account when establishing the addresses and port numbers that RealProxy will use for multicasting:

- Select addresses from a legal range of available addresses. Valid ranges are between 224.0.0.0 and 239.255.255.255. The network administrator should know which multicast addresses are available on your intranet. On the Internet, certain ranges such as the addresses between 224.0.0.0 and 224.0.0.255 are reserved for other uses; see RFC 1700, "Assigned Numbers" for a complete list of restricted addresses.
- You must select enough addresses for the type of file you are multicasting. See "Determining Required Addresses and Port Numbers" for information on selecting the appropriate number. You'll need to know how many bit rates are included in each file that you are multicasting, and set aside the appropriate number.

Although the information in this document will help you calculate the number of addresses and port numbers you'll need for multicasting, you'll still need to consult with your network administrator regarding the actual addresses you'll use.

Determining Required Addresses and Port Numbers

For each file that you are transmitting via multicast, you must calculate the number of addresses you'll need. The number of addresses is based on the number of bit rates in the file. For simple RealVideo files, figuring the number of addresses and port numbers is relatively simple. SureStream files are more complex, as they can contain several bit rates, each with its own number of streams.

Unless you can find out the number of bit rates in the files that you are streaming, you'll have to guess. A safe number is six bit rates per file; the maximum number of bit rates that would be present in a single SureStream file is 14, yet files prepared for multicasts are likely to include only the higher encoding rates. A non-SureStream file would have at most one bit rate and two streams.

Addresses Needed for Back-Channel Multicasts

Bit Rates	Addresses
1	1
2	2
3	3
...	...
n bit rates	*n*

Setting Up Back-Channel Multicasting

Follow the instructions below to set up back-channel multicasting.

➤ To set up back-channel multicasting:

1. In RealSystem Administrator, click **Multicasting**. Click **Back-Channel**.
2. In the **RTSP Port** box, type the port number to which RealProxy will direct its RTSP multicast streams. The value in this box refers to the client's port number. A typical value is `554`.
3. Specify the range of addresses to which you want to multicast streams by filling in the **Address Range** box. RealProxy uses the first available address in this range. If your multicast streams are referenced in SMIL files, you will need one address for each stream.

   Refer to "Determining Required Addresses and Port Numbers" to calculate the exact number of addresses you'll need.
4. Indicate how far multicast packets can travel over a network by typing a value in the **Time to Live** box. Each time a multicast data packet passes through a multicast-enabled router, its Time to Live is decreased by 1. When the value is decremented to 0, the router discards the data packet.

   The value for **Time to Live** can range from `0` to `255`. The larger the Time to Live, the greater the distance a data packet will travel.

The default value of 16 is enough to keep multicast packets within a typical internal network.

Time to Live (TTL) Values

TTL Value	Packet Range
0	Local host
1	Local network (subnet)
32	Site
64	Region
128	Continent
255	World

5. To allow missing packets to be resent to clients that request them, select True from the **Resend** list. This setting is optional. It adds some overhead to the traffic on your network; however, clients receive better quality multicasts.

6. Indicate which clients will be able to view your multicast presentations by configuring the **User List**.

   To require that clients with IP addresses in the User List must connect in multicast mode, set **Deliver Only** to Yes. When this is selected, those clients not configured for multicast will not be able to receive the multicast, and will receive an error message instead. Use this feature when you want to restrict the multicast to a limited number of clients, or if you are multicasting a high-bandwidth presentation and do not want unicast to be an option.

   a. In the **User List** area, select Yes from the **Delivery Only** list.

   b. Click **Add a User List**.

   c. In the **Rule Name** box that appears, type a rule number. The rule number is used by RealProxy for sorting the address rules.

   d. Type the IP Address of the client allowed to receive the multicast in the **IP Address** box. To allow any client to access the multicast, type 0.0.0.0.

   e. Type the subnet mask for the client IP in the **Netmask** box.

      To indicate a single IP address, type 255.255.255.254 in the **Netmask** box. If you typed 0.0.0.0 in the **To** box, type the same thing in the **Netmask** box.

f. Click **OK**.

Repeat Step b through Step f for each set of clients that will be accessing your multicast.

7. Click **Apply**.

Note

Access Control rules are enacted before User List rules. A client that is excluded by Access Control will not be able to connect to any multicasts, regardless of the rules you create here. (IP Access Control is described in Chapter 9, “Limiting Access to RealProxy”.)

Chapter 12

AUTHENTICATING REALPROXY USERS

RealProxy authentication provides a way for you to control the sites visited by RealPlayer. With this feature, you can configure RealProxy to require a valid user name and password before allowing a RealPlayer to access a particular URL.

Overview

You can restrict which users can access content originated from specific locations. You can use this feature to ensure that only certain users can play streaming media that originates outside your network.

You create a list of the sites that all users can visit. If a user requests content from a site not on this list, she is asked for a user name and password. If you have previously created a username and password for that person, she receives the media. If you haven't created a password, or if the user types it incorrectly, she is denied access.

RealProxy identifies requests for secure content by the host name in the URL.

Authentication is a feature also used by some RealServers. As a result, some users may be asked more than once for a user name and password—once by RealProxy, and once by the transmitter RealServer. In each case, the information the user needs to type will be different.

Setting Up Authentication

Setting up the authentication feature has these steps.

1. Identify the sites that all users are allowed to visit.

   To visit any other sites, users must enter their name and password (see the next step).

   Additional Information

   See "Step 1: Identify Permitted Sites".

2. Add user names and passwords.

   These users are permitted to visit sites not listed in the previous step.

   Additional Information

   See “Step 2: Setting Up User Names and Passwords”.

Step 1: Identify Permitted Sites

In this step you choose the sites which all users are allowed to visit without having to supply a user name and password.

Setting Up Permitted Sites

➤ To set up permitted sites:

1. In RealSystem Administrator, click **Security**. Click **Authentication**.
2. From the **Enable Authentication** list, select `Yes`.
3. From the **Realm** list, select `ConnectRealm`.

   If you have set up another Realm, select that name here.
4. From the **Database** list, select `Connect_RN5`.

   If you have set up another database, select that name here.
5. In the **No Authenticate Rules** area, click **Add New**.

   A generic rule name appears.
6. In the **Edit Rule Name** box, type a name for this rule.
7. Click **Edit**.
8. In the **Host** box, type the name of the site to which all users will be permitted access. Use a single asterisk to avoid specificity..

Naming Scheme for Host

Use this form...	...to indicate these sites:
*.org	All sites ending with .org
example.com	The site named www.example.com, including www.sports.example.com.
*.example.com	

Note

Use only one asterisk. For example, `*.*.com` is not allowed.

9. Repeat Step 2 through Step 8 for each site you want to give access to.
10. If you want a user to be able to log in from more than one location and view the same content at more than one location, set **Allow Duplicate IDs** to `Yes`.

    Normally, when **Allow Duplicate IDs** is set to `No`, a user can use only one computer to play streaming media. If a user tries to log in from a second computer, he or she will receive an error message. The user must log out at the first location before being permitted to log in at the second location.
11. Click **Apply**.

Step 2: Setting Up User Names and Passwords

Add the user names and passwords for those users who are allowed to access content. These users will be able to receive streaming media from sites outside the rules you created in "Step 1: Identify Permitted Sites".

Adding User Names and Passwords

Use the following instructions to add to the list of authorized users.

If you are using Windows NT to list the users, use tools supplied by Windows NT instead.

➤ To add user names and passwords:

1. In RealSystem Administrator, click **Security**. Click **Realms**.
2. In the Authentication Realms area, select `ConnectRealm`.
3. Click **Add a User to Realm**.
4. In the new window that appears, type the user's name in the **Name** box.
5. In the **Password** box, give the user's password.
6. In the **Confirm Password** box, type the password again.
7. Click **OK**.
8. Repeat Step 3 through Step 7 for each user you want to add.
9. Click **Apply**.

Optional Authentication Features

Authentication has these optional features:

- Setting Up a New Database
- Creating a New Realm
- Changing RealSystem 5.0 Authentication Passwords

Setting Up a New Database

The databases stores the list of users' credentials. RealProxy includes these database interfaces:

- **Flat file**—The text file method is enabled during installation, as it allows the greatest insight into the access permission structure, but the text file method lacks the flexibility of a full database application.

  It's best to use the text file method only for simple tracking or for troubleshooting the system before linking a full-fledged database to RealProxy. For small-scale data, the text file method is also faster than a full-fledged database.

- **ODBC and MSQL**—The authentication package contains templates for common databases, including mSQL and some ODBC-compliant databases. Users can also work with databases for which templates do not exist, by setting up the data source with the appropriate table structure. The mSQL database is generally used on UNIX.

Setting Up a Database

Use the instructions below to choose the name and type of database that will store users' names and passwords.

➤ To set up a database:

1. In RealSystem Administrator, click **Security**. Click **Databases**.
2. Click **Add New**.

   A generic database name appears in the **Edit Database Name** box.
3. Type a description for the new database in the **Edit Database Name** box.
4. Click **Edit**.
5. From the **Database Type** list, select the data storage method you want to use: `Flat file`, `MSQL`, or `ODBC`.
6. Depending on the database type method you chose, additional information is required.

- **Flat File** needs only the path to the main text file directory. For example, the `con_r_db` directory under the main RealProxy directory. See "Authentication Data Storage".
- **mSQL** has two required names, and three optional items:
    - **Host Name**—IP address or DNS name of computer where database is stored.
    - **Database Name**—Name of the database.
    - **Table Name Prefix**—Prefix used to make field names unique, when used with an existing database.
    - **User Name**—Name required by database application.
    - **Password**—Password required by database application. Re-enter your password in the **Confirm Password** box to ensure you typed it correctly.
- **ODBC** uses the same information as mSQL, but ODBC does not ask for a Host Name. (Refer to "Setting Up Other Types of Data Storage" for further instructions.)

7. After filling out the appropriate values, click **Apply**.

Creating a New Realm

A realm contains information about the type of authentication protocol and the database where the authenticated users' names will be stored. If you will be using Windows NT to authenticate users, the realm lists the type of NT authentication and the NT administrator-defined group name.

Authentication Protocols

RealProxy has three methods of authenticating the identity of visitors. Each realm can use only one authentication method.

- **RealSystem 5.0**—also called "RN5", it is RealNetworks' own authentication protocol. This is a more sophisticated protocol than Basic authentication. It provides better security than Basic because it does not send the password in a manner that can be reversed.

  If the clients that will be accessing content on your RealProxy are RealPlayer version 5.0 and earlier, be sure to use the RealSystem 5.0 style.

- **Windows NT LAN Manager**—this method allows RealProxy to use the existing NT database of user groups and permissions. It also allows access control of content via NTFS file permissions. This protocol uses Windows NT authentication.

  This method is only available to systems using Windows NT, and requires that RealProxy itself be installed on an NT Server. For authenticating content, it also requires Microsoft Internet Explorer and RealNetworks RealPlayer.

- **Basic Authentication Protocol**—encodes the user's name and password with the Base64 algorithm and sends it to RealProxy, which then decodes the password and verifies it.

Setting Up a Realm

Use the instructions below to create a realm.

➤ To create a realm:

1. In RealSystem Administrator, click **Security**. Click **Realm**.
2. In the Authentication Realms area, click **Add New**.

   A generic realm name appears in the Edit Realm Description box.
3. In the **Edit Realm Description** box, type a name for this realm.
4. Click **Edit**.
5. In the **Realm ID** box, type a name. You will use this name in other areas of RealSystem Administrator, so make a name that is meaningful to you. The Realm name may also appear to users as part of the name and password prompt.
6. In the **Authentication Protocol** list, select the authentication method you want to use for this realm, based on the descriptions in "Authentication Protocols" earlier in this chapter.

   If you choose `Basic` or `RealSystem 5.0`, you will also need to select a database in which the names and passwords of authenticated users will be stored. Refer to "Setting Up a Database".

   If you choose `Windows NT Lan Manager`, you do not need to select a database—instead, RealProxy will use the NT list of names. Use the additional steps shown here:

   a. Type the appropriate provider in the **Provider** list, such as `NTLM`.

b. Type the Group name in the **Group** box.

7. Click **Apply**.

Changing RealSystem 5.0 Authentication Passwords

When you use the RealSystem 5.0 authentication protocol, RealProxy stores all passwords in an encrypted format. Passwords can be entered and changed through RealSystem Administrator. If you want to change the passwords manually, without using RealSystem Administrator, you can use the supplied password command line utility. It is located in the RealProxy `Bin` directory.

You can also use these instructions as a basis for writing your own CGI scripts and Web pages to accomplish the same purpose automatically.

➤ To use the password tool manually:

1. At a command line, in the Bin directory, type the following:

   ```
   mkpnpass username realm
   ```

   where:

   username is the user name exactly as it is entered or will be entered in the authentication database or text file.

   realm is the value of the `Realm` variable specified in the relevant list.

   For RealSystem Administrator users, use the value of the `Realm` variable in the `RealAdministrator_Files` list within the `FSMount` list in the configuration file. (You must open the configuration file itself to see this value.)

2. A password prompt appears, followed by a prompt to type the password again.

   The resulting encrypted password is displayed on the screen.

   RealProxy encrypts passwords with the MD5 hashing algorithm. It uses the form `MD5("username:realm:new_password")`. On BSD systems and some other UNIX systems, you can generate these passwords with the following command:

   ```
   echo -n "username:realm:new_password" | md5
   ```

3. Add the resulting encrypted password into the appropriate field of the database:

   - For flat text files, place it in the password field of the `User` directory (see “Users Directory”).

- For databases, place it in the password field of the Users table (see "Users Table").

Authentication Data Storage

This section describes the methods for storing user name and password data. The information can be stored in either a series of text files or in a database. Templates for common databases are created during installation, that correspond to the database methods listed in "Setting Up a New Database".

- **Text file storage**—this method uses a combination of directory structure and text files to achieve a sensible data storage method. It is the default method. See "Using Text Files for Authentication Data" for details.
- **Database templates**—the supplied templates use a similar structure to the text file method, in a more familiar database format. Refer to "Using a Database for Authentication Data" for more information.

Using Text Files for Authentication Data

The default configuration uses the text file storage method to provide storage for all the realms.

The following directories contain the text files which store data. The center letter indicates the authentication protocol: `r` is for RN5, `b` is for Basic.

Supplied Data Storage Directories

Directory Name	Data Storage for the following type of information
`adm_b_db`	RealSystem Administrator User Authentication
`con_r_db`	Connection Authentication

The contents of the directories are given in the table below.:

Text File Storage Directory Structure

Directory	Contents	File or Directory Description
Main directory (`con_r_db` or `adm_b_db`)	`ppvbasic.txt`	The text file indicates to RealProxy that this is the storage area for the list of authenticated names.
`users`	(initially blank)	Files in this directory list the clips and permission types.

Text File Storage Directory Structure

Directory	Contents	File or Directory Description
`logs`	`accesslog.txt`	See below for a description.
`redirect`	(initially blank)	For player validation, files contain an URL to which to send the client if redirection is necessary.

When RealProxy creates the file structure, it creates the `ppvbasic.txt` file. The second and subsequent times you start the RealProxy, the program looks for this file. If the file does not exist, it recreates the directory structure.

Warning

Do not delete the `ppvbasic.txt` file! If you delete the `ppvbasic.txt` file, RealProxy will rewrite the directories and will erase their prior content.

Users Directory

The files in this directory are named *`username`*, where *`username`* is the user name. This directory contains one file per registered user.

The first line of each file has the following format:

password;*uuid*;*uuid_writeable*

where:

password	When user authentication is in use, this stores the password. Otherwise shows an asterisk (*). Note: Passwords are encrypted. To change them manually, see “Changing RealSystem 5.0 Authentication Passwords”.
uuid	In player validation, stores playerID. In user authentication, an asterisk (*) appears in this field.
uuid_writeable	A flag set and used by RealProxy: 0 playerID is in database 1 record created, but playerID is not yet registered

Note

If you manually edit the files, be sure that any blank (or unused) fields use an asterisk (*) as a placeholder. Do not use a space for a placeholder.

Logs Directory

This directory contains accesslog.txt, which is not created until authentication is enabled and the first user connects to RealProxy.

Accesslog.txt

Each line of accesslog.txt describes the result of an attempt to view a clip. Syntax of this file:

status;userid;uuid;ip;url;access_type;permission_on;start_time;end_time;total_time; why_disconnect

where:

status	Result of user's attempt to connect: 0 access to clip granted 1 denied
userid	Unique name of up to 50 characters.
uuid	Stores playerID.
ip	IP address from which user is attempting to connect
url	Secured clip user is attempted to access.
permission_type	Event value.
permission_on	Always 0.
start_time	Time/date clip started playing.
end_time	Time/date clip stopped playing.
total_time	Total time clip played.
why_disconnect	Reasons for disconnection: 0 client disconnected voluntarily 1 server access expired

Using a Database for Authentication Data

This section describes the structure of the database templates included with RealProxy.

To set up the database, see "Setting Up Other Types of Data Storage".

The database templates include these tables:

- **Users table**—Lists who is registered and with what access.
- **Access_log table**—Used by this feature.

Users Table

Gives the list of user names and passwords.

Users Table

Field	Description
userid	User name of up to 50 characters. Ties to permissions table.
password	In user authentication, this stores the password. Otherwise blank. Note: Passwords are encrypted. To change them manually, see “Changing RealSystem 5.0 Authentication Passwords”.
uuid	In player validation, stores clientID. In user authentication, an asterisk (*) appears in this field.
uuid_writeable	A flag set and used by RealProxy: 0 clientID is in the database 1 the record has been created but the clientID is not yet registered with RealProxy.

Access_log Table

Shows which restricted sites have been accessed.

Access_log Table

Field	Description
status	Result of user’s attempt to connect: 0 access to clip granted 1 denied
userid	Unique name of up to 50 characters.
uuid	Stores player ID.
ip	IP address from which user is attempting to connect.
url	Secured clip user is attempted to access.
permission_type	Event value.
permission_on	This field is always 0.
start_time	Time/date clip started playing.
end_time	Time/date clip stopped playing.
total_time	Total time clip played.
why_disconnect	Reason for disconnection: 0 client disconnected voluntarily 1 server access expired

Setting Up Other Types of Data Storage

Support for two types of databases is included: ODBC and MSQL.

➤ To set up your Windows computer for ODBC compliance:

1. On the **Start** menu, point to **Settings**, and click **Control Panel**.
2. Double-click **32bit ODBC.**
3. On the **System DSN tab**, click **Add**.
4. Select your ODBC driver from the list of drivers and click **Finish**.
5. In the **ODBC SQL Server Setup** dialog box, type the data source name. Click **Select**.
6. Type or browse for the path to your database file and click **OK**.
7. Click **OK** to exit the ODBC Data Source Administrator.

You must now tell RealProxy where to find your database.

➤ To set up the supplied database application on UNIX:

1. At a command line, start the database by typing the following:

   ```
   ./msql2d &
   ```

2. Create the database by typing the following:

   ```
   ./msqladmin create databasename
   ```

3. Note that whatever you type for *databasename* will need to match the database cited in the Databases list.
4. Create the tables using the database text file by typing the following:

   ```
   .msql -h localhost databasename < ppvdemo.db
   ```

   Be sure to include the less-than sign (<).

Chapter 13

MONITORING REALPROXY ACTIVITY

RealProxy includes a monitoring page within RealSystem Administrator, which you can use to view the number of clients currently connected. This chapter gives brief instructions in using this feature.

To generate reports of historical activity, see Chapter 14, “Tracking RealProxy Activity”.

Using RealSystem Administrator

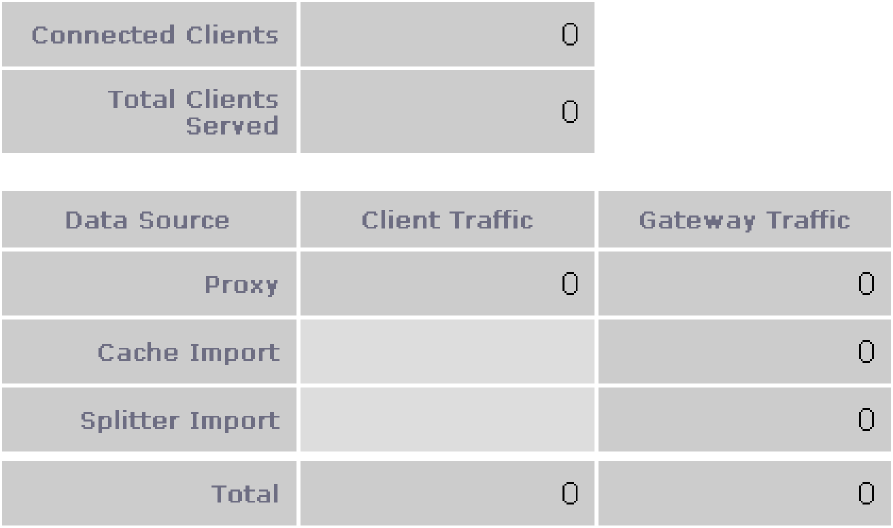
RealSystem Administrator includes a section where you can view RealProxy activity.

➤ To view RealProxy activity via RealSystem Administrator:

In RealSystem Administrator, click **Monitor**. The monitor page appears in the right-hand frame. It dynamically updates to show information about the number of connections, and so on.

Additional information about the information shown is available on the monitor page itself.

Monitor in RealSystem Administrator



Connected Clients	0
Total Clients Served	0

Data Source	Client Traffic	Gateway Traffic
Proxy	0	0
Cache Import		0
Splitter Import		0
Total	0	0

The significance of these numbers is shown below:

- **Connected Clients**—shows how many clients are currently using RealProxy.
- **Total Clients Served**—gives the number of clients that have used RealProxy since it was last started.
- **Data Source**—shows the RealProxy features used to deliver the requests.
- **Client Traffic**—lists the number of clients whose requests were delivered via the particular Data Source method, in bits per second.
- **Gateway Traffic**—shows the amount of bandwidth consumed by each Data Source type, in bits per second.

Chapter 14

TRACKING REALPROXY ACTIVITY

RealProxy can create reports of historical data that let you see trends and gather information. This information is stored in the proxy log. Any error messages are recorded in the error log. This chapter shows how to read those logs, and how to change where the log files are stored.

Proxy Log

The proxy log records the IP addresses of the clients that have connected, the clips they listened to, the times of day they connected, and much more. New information is always appended to the end of the proxy log.

Reading a Proxy Log

To read the contents of the proxy log, you must first look up the values of Logging Style in RealSystem Administrator, as this determines how much information is present in the proxy log. At installation, Logging Style is set to `3`.

Logging Style provides information about RealProxy clip-serving activity.

Once you know the values of Logging Style, view the proxy log by opening `proxy.log` (Windows) or `proxy` (UNIX) file in a word processor or text editor.

Proxy Log Format

RealProxy stores information about each clip it serves in a separate record. Each record is delimited by a new line. Fields within each record are separated by spaces.

One record is created for every clip served; if the client requests a presentation that includes several clips, one record is created for each clip in the presentation.

The fields that appear within each record depend on the settings for Logging Style. The complete syntax of each record, assuming Logging Style is gathering all possible information (Logging Style is 5) is shown:

client_IP_address - - [*timestamp*] "GET *filename protocol/version*" *HTTP_error_code bytes_sent* [*client_info*] [*client_GUID*] *file_size file_time sent_time resends failed_resends* [*stream_components*] *start_time server_address average_bitrate packets_sent presentation_id* [*proxy_info*]

Note

Although in the rest of this manual, square brackets indicate optional material, the square brackets shown in the proxy log actually appear within proxy log records.

The following table lists the format for each proxy log record:

Proxy Log Format

Proxy Log Field	Description
client_IP_address	IP address of client, such as 123.45.123.45
- -	Two hyphens for compatibility with standard Web server log formats.
timestamp	Time that client accessed the file in the format: *dd/Mmm/yyyy:hh:mm:ss TZ* where *TZ* is the time zone expressed as the number of hours relative to the Coordinated Universal Time (Greenwich, England) and is relative to the server. For example: [31/Oct/1996:13:44:32 -0800]
"GET *filename* or "GET *URL*	Requests for PNA will show the file name (and path) requested by the client. Requests for RTSP will show the complete URL, beginning with rtsp://. If the client requests a file that doesn't exist, UNKNOWN appears in place of a file name.

Proxy Log Format (continued)

Proxy Log Field	Description	

protocol/version”	Application-layer protocol used to send the clip to the client. Possible values are:
	`RTSP`
	`PNA`
	In addition, a letter at the end of the string indicates which transport type was used:	

	`(blank)`	UDP connection
	T	TCP connection
	`M`	Multicast
	For example, `PNAT` means that the clip was sent using the PNA protocol over a TCP connection. The version number indicates the edition of the protocol.	
HTTP_status_code	Return code using HTTP standard error codes. Usually returns `200`.	
bytes_sent	Number of bytes transferred to the client.	

Proxy Log Format (continued)

Proxy Log Field	Description	
[*client_info*]	Describes the version and type of client being used. Client information appears in the following format, [*platform version client type dist_code language CPU*] If client information can't be gathered (the request came from a client that chose not to send statistics, or from a browser connecting to RealSystem Administrator pages), `UNKNOWN` appears within the brackets.	
	Field	Description
	platform	Operating system RealPlayer runs on-Win16, WinNT, Mac, and so on.
	version	Operating system version number.
	client	Version number of RealPlayer.
	type	Type of RealPlayer.
	dist_code	Distribution code of RealPlayer.
	language	Language setting in RealPlayer.
	CPU	Type of processor on which the client is running. If the processor does not have a hardware Floating Point Unit, the string "no-FPU" is appended to the end of the CPU field with no delimiter. For example: `Win95_4.0_3.0.0.19_play32_PN01_EN_586`
	RealAudio Player version 1.0 shows only two fields for [*client_info*]. They are *platform* and *client*.	
[*client_GUID*]	Unique ID generated during RealPlayer installation that enables you to track details for individual clients. If client information can't be gathered (the request came from a client that chose not to send statistics, or from a browser connecting to RealSystem Administrator pages), `UNKNOWN` appears within the brackets. If the user elects to suppress this information, this field will show a series of zeroes: `00000000-0000-0000-0000-000000000000` instead of a unique identifier. Refer to "Omitting Client Identifiers". Included when `Logging Style` is set to `2` or higher.	

Proxy Log Format (continued)

Proxy Log Field	Description
`[Stat1]` (see the "Statistics Type 1 Information" table)	Connection statistics sent by the client when it completes playing a clip (see the "Statistics Type 1 Information" table). When the client blocks connection statistics, the field is replaced by `[UNKNOWN]`. Note that there is no space between the closing square bracket of this statistics type and the opening square bracket of the next statistics type. Included when `Stats Mask` is `1`, `3`, `5`, or `7`.
`[Stat2]` (see the "Statistics Type 2 Information" table)	Extended connection statistics sent by the client when it completes playing a clip (see the "Statistics Type 2 Information" table). When the client blocks connection statistics, the field is replaced by `[UNKNOWN]`. Note that there is no space between the closing square bracket of this statistics type and the opening square bracket of the next statistics type. Included when `Stats Mask` is `2`, `3`, `6`, or `7`.
`[Stat3]` (see the "Statistics Type 3 Information" table)	Actions taken by the visitor while playing the clip (see the "Statistics Type 3 Information" table). When the client preferences are set to block statistics, this field is replaced by `[UNKNOWN]`. Note that there is no space between the closing square bracket of the previous statistics type and the opening square bracket of this statistics type. Included when `Stats Mask` is `4`, `5`, `6`, or `7`.
file_size	Reserved for future use. Currently this information is not recorded by RealProxy. Included when `Logging Style` is set to 1 or higher.
file_time	Reserved for future use. Currently this information is not recorded by the RealProxy. Included when `Logging Style` is set to `1` or higher.
sent_time	Total length, in seconds, of the media sent to the client. Included when `Logging Style` is set to `1` or higher.
resends	Number of packets successfully resent because of transmission errors. Included when `Logging Style` is set to `1` or higher.
failed_resends	Number of packets not successfully resent in time to correct transmission errors. Included when `Logging Style` is set to `1` or higher.

Proxy Log Format (continued)

Proxy Log Field	Description
[stream_ components]	Type of material sent, indicated in the following pattern: `RealAudio RealVideo Event RealImage` `1` shows that the stream includes this type, `0` indicates that it does not. Thus, a stream that included RealVideo and RealAudio but no events or RealImages would appear in the proxy log as: `1 1 0 0`. Included when `Logging Style` is set to `3` or `4`.
start_time	Timestamp of start time. Included when `Logging Style` is set to `3` or `4`.
server_address	IP address where clip came from. This may be the transmitterRealServer, a RealServer which is acting as a receiver, or another RealProxy which is acting as a receiver. In cache mode, RTSP requests will show the cache's address (usually 127.0.0.1). To find the address of the transmitter, look in the GET field (see “`GET filename` or “`GET URL`). Included when `Logging Style` is set to `3` or `4`.
average_bitrate	Average bitrate of clip. This field always shows `0`. Included when `Logging Style` is set to `4`.
packets_sent	Number of packets sent. Included when `Logging Style` is set to `4`.
presentation_id	Number shown by all clips in the same SMIL presentation. The SMIL file itself is also included in the log, and shares the number as well. The number is assigned by RealProxy at the time of transmission. Included when `Logging Style` is `5`.
[proxy_info]	Displays information about the type of proxied stream (always included):

Value	Meaning
`Demand Pass-Through`	The proxied stream was an on-demand clip, and it was sent in passthrough mode.
`Live Pass-Through`	The proxied stream was a live clip, and it was sent in passthrough mode.
`Live Split`	The proxied stream was a live clip, and it was sent via push splitting.
`Demand Cache Hit`	The proxied stream as an on-demand clip, and RealProxy served it from the media cache.
`Unknown`	Clip type and delivery were of unknown type.

StatsMask Results

The information gathered by each of the three Statistics Types are listed in this section. `Stat1` and `Stat2` report information about the RealAudio portion of a clip. Even if a clip includes both RealAudio and RealVideo, these statistics report solely RealAudio information. `Stat3` reports information about visitor and client behavior while playing all types of clips or presentations.

When Stats Mask is `0`, two square brackets (`[]`) appear instead of the `Stat1`, `Stat2`, and `Stat3` sections.

Stat1 Syntax

Statistics Type 1 gathers basic information about how successfully audio clips were received by the client. It also tells what the client used to decode the audio portion of the clip.

Syntax of this portion of the access log record:

`[Stat1:` *packets_received out_of_order missing early late audio_format*`]`

The table below gives the information collected by this statistic type:

Statistics Type 1 Information

Field	Description
packets_received	Total number of packets received by the client.
out_of_order	Number packets received by the client out of order. These packets are reordered as they are being played by the client.
missing	Number of packets requested by the client, but that the client did not receive.
early	Number of requested packets received too early by the client.
late	Number of packets received too late by the client.
audio_format	Name of the decoder used to play the clip. Possible values are: `sipr` RealAudio 5.0 formats `dnet` RealAudio 3.0 formats `28.8` RealAudio 2.0 28.8 format `lpcJ` RealAudio 2.0 14.4 format `cook` RealAudio G2 format

Stat2 Syntax

Statistics Type 2 provides details about the success of clip delivery, giving information about bandwidth requests. Re-sent packets are described in detail here. It identifies which transport type was used to make the connection and which video decoder played the clip. This set of statistics uses the following format:

[Stat2: *bandwidth available highest lowest average requested received late rebuffering transport startup format*]

The table below explains what information is collected by this statistic type:

Statistics Type 2 Information

Field	Description
bandwidth	Bandwidth of the clip, in bits per second.
available	Average bits per second available to the user while the clip was playing.
highest	Highest time between the client resend packet request and the packet resend arrival, in milliseconds.
lowest	Lowest time between the client resend packet request and the packet resend arrival, in milliseconds.
average	Average time between the client resend packet request and the packet resend arrival, in milliseconds.
requested	Number of resend packets requested by the client.
received	Total number of re-sent packets received by the client.
late	Number of re-sent packets received by the client too late.
rebuffering	Rebuffering percentage for the clip.
transport	Transport type for the connection. Values are: 0: UDP 1: TCP 2: IP Multicast 3: PNAviaHTTP
startup	Time when the client receives the first clip data, in milliseconds. The data may arrive before the clip starts playing.
format	Name of the decoder used to play the clip. Possible values are: sipr RealAudio 5.0 formats dnet RealAudio 3.0 formats 28.8 RealAudio 2.0 28.8 format lpcJ RealAudio 2.0 14.4 format cook RealAudio G2 format

Stat3 Syntax

Statistics Type 3 provides detailed information about viewer action while listening or viewing clips. It addresses advanced features of the implementation, notably ads and image maps. You can find out at what point in the clip a viewer clicked on an image map or stopped watching the clip.

If Stats Mask is configured to gather statistics type 3 (Stat3), note that the access log file size will grow rapidly. If you configure Stats Mask to collect this information, be sure to review the log file frequently. This statistics type uses the following format:

```
[Stat3:timestamp|elapsed_time|action|;]
```

Records of activity are separated by a semicolon (;) and are in the following form:

```
timestamp|elapsed_time|action|;
```

Thus, the Stat3 record of a visitor pausing, resuming play, and watching to the clip's end would look like the following:

```
[Stat3:4360|2107|PAUSE|;8401|2107|RESUME|;12608|6321|STOP|;]
```

The table below gives the format of the Stat3 records:

Statistics Type 3 Information

Field	Description
timestamp	Time in milliseconds when action occurred. It is relative to the connect time of the client.
elapsed_time	Elapsed time of the clip when the behavior occurred, given in milliseconds.

Statistics Type 3 Information (continued)

<table>
<tr><th>Field</th><th colspan="4">Description</th></tr>
<tr><td rowspan="14">*action*</td><td colspan="4">The visitor’s or client’s behavior, where values are the following:</td></tr>
<tr><td rowspan="7">CLICK</td><td colspan="3">Visitor clicked on the image map. Further information includes:</td></tr>
<tr><td>*x-coord*</td><td colspan="2">Horizontal coordinate of click.</td></tr>
<tr><td>*y-coord*</td><td colspan="2">Vertical coordinate of click.</td></tr>
<tr><td rowspan="4">*action*</td><td colspan="2">Action that occurred. This is one of the following:</td></tr>
<tr><td>PLAYER="*url*"</td><td>The URL of the link the viewer clicked, as used in the client</td></tr>
<tr><td>URL="*url*"</td><td>The URL of the link the viewer clicked, as used in the Browser.</td></tr>
<tr><td>SEEK="*destination*"</td><td>The seek destination point, in milliseconds.</td></tr>
<tr><td>PAUSE</td><td colspan="3">The visitor paused the client.</td></tr>
<tr><td>RESUME</td><td colspan="3">Resume play after a pause, seek or stop.</td></tr>
<tr><td>SEEK</td><td colspan="3">The seek destination point, in milliseconds.</td></tr>
<tr><td>STOP</td><td colspan="3">End of clip reached.</td></tr>
<tr><td>RECSTART</td><td colspan="3">RealPlayer Plus began recording the clip.</td></tr>
<tr><td>RECEND</td><td colspan="3">RealPlayer Plus stopped recording the clip.</td></tr>
</table>

LoggingStyle Results

The format of the proxy log under each of the different Logging Style values is shown in the table below:

Logging Style Effect on Proxy Log

Logging Style value	Individual record format
0	*client_IP_address* - - [*timestamp*] "GET *filename protocol/version*" *HTTP_status_code bytes_sent* [*client_info*] [*client_GUID*] [*proxy_info*]
1	*client_IP_address* - - [*timestamp*] "GET *filename protocol/version*" *HTTP_status_code bytes_sent* [*client_info*] [*client_GUID*] *file_size file_time sent_time resends failed_resends* [*proxy_info*]
2	*client_IP_address* - - [*timestamp*] "GET *filename protocol/version*" *HTTP_status_code bytes_sent* [*client_info*] [*client_GUID*] *file_size file_time sent_time resends failed_resends* [*proxy_info*]

Logging Style Effect on Proxy Log (continued)

Logging Style value	Individual record format
3	*client_IP_address* - - [*timestamp*] "GET *filename protocol/version*" *HTTP_status_code bytes_sent* [*client_info*] [*client_GUID*] *file_size file_time sent_time resends failed_resends* [*stream_components*] *start_time server_address* [*proxy_info*]
4	*client_IP_address* - - [*timestamp*] "GET *filename protocol/version*" *HTTP_status_code bytes_sent* [*client_info*] [*client_GUID*] *file_size file_time sent_time resends failed_resends* [*stream_components*] *start_time server_address average_bitrate packets_sent* [*proxy_info*] [*proxy_info*]
5	*client_IP_address* - - [*timestamp*] "GET *filename protocol/version*" *HTTP_status_code bytes_sent* [*client_info*] [*client_GUID*] *file_size file_time sent_time resends failed_resends presentation_id* [*proxy_info*]

Information Recorded by RealServer

If you are also managing a transmitter RealServer, you know that similar information is recorded in the transmitter's access log. Information about client requests is stored in both the proxy log and the transmitter's access log. Each Server's settings are independent of each other, and the appropriate information is recorded in each Server's log file. For example, RealProxy may be configured to record Logging Style 0, and RealServer may be collecting all the information of Logging Style 5.

Customizing Information Reported by the Proxy Log

RealProxy uses the following settings for the proxy log (you can view these in RealSystem Administrator by clicking **General Setup**>**Logging**):

- **Logging Style**—At installation, this is set to 5.
- **Disable Client GUIDs**—This setting gathers client software identification.
- **Stats Mask**—The default value is 3.
- **Log Rolling Frequency**—Settings for creating new log files at specified intervals. See "Log File Rolling".
- **Log Rolling Size**—Settings for creating new log files at specified sizes. See "Log File Rolling".

- **Proxy Log File**—RealSystem Administrator will place files in the `Logs` subdirectory of the main RealProxy directory. The default file name of the proxy log file is `rmaccess.log` (Windows) or `rmaccess` (UNIX). The directory (if any) typed here can be absolute or relative to the base path of the main mount point.

  If **Proxy Log File** is blank, RealServer records access information in the `proxy.log` or `proxy` file located in the same directory as the RealServer executable file.

  The name of the proxy file will be different if Log File Rolling is enabled; see “Log File Rolling”.

To customize the information gathered in the proxy log, you must first decide what types of information you want to gather. Then make the appropriate changes to Logging Style, which collects information about RealServer activity, and to Stats Mask, which gathers statistics about what arrived at the client and viewer behavior while playing the clips.

To gather information with the proxy log, you must first decide what types of information you want to gather. Then make the appropriate changes to Logging Style.

Changing Information Gathered with Stats Mask

Stats Mask supplies more detailed information to the access log. This variable is optional. For a complete description of information collected by each statistics type, and the syntax of the types as they appear in the access log, see the “Statistics Type 1 Information” table, the “Statistics Type 2 Information” table, and the “Statistics Type 3 Information” table.

If you omit a value for Stats Mask, RealServer uses the default value of 3 (gather statistics types 1 and 2).

Collecting Combinations of Stats Mask Information

To gather this information...	...set Stats Mask to this value	Statistics Type 1	Statistics Type 2	Statistics Type 3
No additional statistics	0			
Statistics type 1 only	1	•		

(Table Page 1 of 2)

Collecting Combinations of Stats Mask Information (continued)

To gather this information...	...set Stats Mask to this value	Statistics Type 1	Statistics Type 2	Statistics Type 3
Statistics type 2 only	2		•	
Both statistics types 1 and 2	3	•	•	
Statistics type 3 only	4			•
Both statistics types 1 and 3	5	•		•
Both statistics types 2 and 3	6		•	•
All statistics (types 1, 2, and 3)	7	•	•	•

(Table Page 2 of 2)

Tip

If Stats Mask is configured to gather statistics type 3, the access log file size will grow rapidly. If you configure Stats Mask to collect this information, be sure to review the log file frequently, or use log file rolling.

Not all versions of RealPlayer supply the information requested by Stats Mask; Statistics type 2 is supplied by RealAudio Player versions 3.0 and later, and Statistics type 3 is supplied by RealPlayer versions 5.0 and later.

Gathering Information with Logging Style

Logging Style has six options, styles 0 through 5. Styles 0 through 4 each includes information of the logging styles with lower numbers. Thus, Logging Style 3 collects the information that's collected by styles 0, 1, and 2, as well as the material gathered by style 3. Logging Style 5 consists of the fields in Logging Style 2, plus the *presentation_id* field.

A list of information gathered by each value is given below.

Logging Styles 0, 1, and 3 contain some additional information, as described in "Proxy Log Format"

Information Collected by Logging Style

To gather this information...	...set LoggingStyle to this value
Bytes sent	0 or higher
Clip name including path	0 or higher

Information Collected by Logging Style

To gather this information...	...set `LoggingStyle` to this value
Client IP address and platform information	`0` or higher
Timestamp	`0` or higher
Packets successfully and unsuccessfully re-sent	`1` or higher
Protocol (RTSP or PNA)	`1` or higher
Send time (total media sent in seconds)	`1` or higher
Transport method (TCP, UDP) and version	`1` or higher
Client ID	`2` or higher
Server IP Address	`3` or `4`
Stream components	`3` or `4`
Timestamp for start time	`3` or `4`
Average bitrate	`4`
Packets sent	`4`
Common presentation identifier	`5`

Omitting Client Identifiers

Normally, every proxy log record displays a unique client identification number for each user. However, both users and administrators have the option to omit this information from proxy log records.

If a user elects to withhold his software's unique client number, a string of zeroes appears instead: `[00000000-0000-0000-0000-000000000000]`.

RealServer's default behavior is to use client identifiers, when available. It will show zeroes for those users who have opted to suppress their client software identifiers.

Regardless of the user's setting, you can instruct RealServer to always show the string of zeroes instead of the actual client identifier. If you choose this option, all proxy log records show zeroes, rather than the actual client identifiers. (This applies only to the logging styles that collect data for the [*client_GUID*] field—logging styles 2 and higher.)

There is no way to override the client's setting, should the user choose to send only zeroes.

➤ To disable collection of client identifiers:

1. In RealSystem Administrator, click **General Setup**. Click **Logging**.
2. From the **Disable Client GUID** list, select `No`.

3. Click **Apply**.

Log File Rolling

Proxy log files can grow indefinitely as they accumulate data. To keep log files to a manageable size, you can limit the proxy log to a weeks's worth of information or a certain file size, and RealProxy will begin a new log file when the limit is reached.

Log file rolling applies only to proxy log files.

➤ To set up log file rolling:

1. In RealSystem Administrator, click **General Setup**. Click **Logging**.
2. Indicate where log files should be stored by giving the path and file name in the **Proxy Log Path** box.
3. Decide whether to limit the log files by time period or by size.
   - To limit by time period, choose the period from the **Log Rolling Frequency** list. You can save by the hour, day, week, or month.

     In the **Log Rolling Interval** box, type the number of time periods. For example, if you chose **Days** from the **Log Rolling Frequency** list and typed `4` in the Log Rolling Interval box, RealProxy will start a new proxy log every 4 days.
   - To limit by file size, type a number in the **Log Rolling Size** box. Specify the size in megabytes.

   If you have values in all three boxes, RealProxy will use the size or time period that is reached first.
4. When you're done, click **Apply**.

Rolled log files are named with the following format:

name`.log.`*datestamp*

where:

name Name of the regular log file. The name for proxy logs is taken from the `LogPath` setting (usually `rmaccess`).

`log` The log file extension.

datestamp The date stamp, in the following format:
YYYYMMDDHHMMSS
where:

YYYY	Year.
MM	Two digits of the month.
DD	Date, in two digits. January would be 01.
HH	Hour
MM	Minutes
SS	Seconds

Disabling Log File Rolling

Choose **Never** from the **Log Rolling Time Period** list, and type `0` (zero) for the **Log Rolling** size.

Error Log

The error log contains both information and error messages about server operation. By looking for patterns of errors, you can troubleshoot and correct possible problems on your site.

View the text of the error log using a word processor or text editor.

The error log is an excellent tool for troubleshooting any problems that may arise with your RealProxy. An entry is made to the error log only when an error occurs. If no errors occur, this file will not exist.

Error messages relating to RealProxy activity appear in the error log. The error log is created when the first error occurs.

If you have an error message in the error log that refers to a fatal error, contact the RealNetworks Technical Support Department for assistance.

➤ To customize where RealProxy creates the error log:

1. In RealSystem Administrator, click **General Setup**. Click **Logging**.
2. In the **Error Log Path** box, type the path and name you want to use for the error log. The default location is the `Logs` directory of the main RealProxy directory, and the default file name is `rmerror.log`.
3. When you have finished making changes, click **Apply**.

Error Log Format

The error log records client connections and RealProxy errors. Each time an error is generated by RealProxy, a record is created in the error log. The error log path is stored in the same directory as the proxy log, indicated by the `LogPath` variable.

Syntax of the file is as follows:

`***`*`date time servername(process_ID)`*`:` *`error_message`*

where entries are defined below:

Error Log Syntax

Entry	Meaning
`***`	Three asterisks indicate an error. Informational messages are not preceded by asterisks.
date	Date on which the error occurred. Given in the form `d-Mmm-YY`.
time	Time the error occurred, according to RealProxy. Given in the form `HH:MM:SS:TT.hhh`
servername(process_ID)	The server name, followed by the process ID in parentheses.
error_message	Text of error message

Chapter 15

TROUBLESHOOTING REALPROXY

This chapter covers general troubleshooting steps to take if something goes wrong in RealProxy.

Overview

If you encounter problems when running RealProxy, you can narrow down the problem with the following tasks:

- Determine scope of the problem—is the problem with clients connecting to RealProxy, or with RealProxy connecting to the transmitter RealServer?
- Check the error logs—messages in the error log file (or files, if you've set up log file rolling) will direct you to the problem. For instructions on how to interpret the log file formats, see "Error Log".

General Troubleshooting Steps

These steps are good ones to check whenever you have trouble with any RealProxy features.

Step 1: Make sure RealProxy is running.

When you started RealProxy, were there any error messages? If so, look up the message in the index of this document.

I can't start RealProxy at all.

There are several possible causes of RealProxy not starting:

- If you are running Windows NT, RealProxy is automatically installed as a service, which means that it runs automatically. If it is installed as a service, and you try to start RealProxy using any other method, it appears not to start. An error message may appear. To find out if it is already running, click **Start>Settings>Control Panel>Services** and look for `RMServer` in the list; the word “Started” in the Status field indicates that it’s running.

- If you are running UNIX, make sure you are logged on with the correct user name. RealProxy requires the use of port 554, and you must be logged on as root in order to access this port. The error message “Could not open port 554” appears on screen when you try to start.
- Your license may have expired, or the license file may have become corrupted. Messages such as the following will indicate this problem.

  “Error - RTSP proxy not licensed for use. Either no license key exists, or the license key present is invalid.”

  “Error - PNA proxy not licensed for use. Either no license key exists, or the license key present is invalid.”
- The error message “Could not open port 7070” indicates that either other software is using the port, or RealProxy could not bind to the necessary address. See the next item for instructions on binding to a particular address.
- You may need to bind RealProxy to a specific IP address. This is often the case when you receive the error message “Server not responding properly: Heartbeat check disabled”. (Heartbeat check is a self-monitoring feature which ensures that the RTSP port is available.) See “Binding to a Specific Address”.
- RealProxy may be bound to an address that doesn’t exist. Using the information in “Binding to a Specific Address”, either delete the `IPBindings` section, or change it to use the single `0.0.0.0` address.

Binding to a Specific Address

To bind to an address, open the configuration file in a text editor. If this is a new installation of RealProxy, and the configuration file has not been customized, you will need to add the following text to the configuration file. The configuration file is named `rmserver.cfg`, and is located in the RealProxy main directory. Add this text to the end of the file:

```
<List Name="IPBindings">
  <Var Address_01="0.0.0.0"/>
</List>
```

The address `0.0.0.0` binds RealProxy to all IP addresses available on this machine. You can substitute the machine’s actual address, instead. Note that if you bind to an actual address, you must also bind to the loopback address (`127.0.0.1`).

Determining the IP Address of Your Computer

Use the appropriate method for your operating system:

- **Windows NT**—Click **Start>Run>Command Prompt**. At the prompt that appears, type `ipconfig`.
- **UNIX**—Most UNIX platforms will report the IP address if you use the command `ifconfig`.

When I click the RealProxy icon, the command window appears briefly but then disappears.

Rather than remaining visible, the window closes if RealProxy encounters an error. Use the following steps to find out what the error is:

1. Open a command prompt.
2. Move to the `Bin` directory.
3. Start RealProxy by typing

   ```
   Bin\rmserver rmserver.cfg
   ```

RealProxy will attempt to start, and any error messages will appear on screen. The most frequent causes of this type of problem are an expired license or conflicting port use.

Also, compare your system date to the Issue and Expire date shown on the **About** page of RealSystem Administrator, and make sure your system date is accurate.

RealProxy is running, but many features have stopped working.

If your license files have expired, RealProxy runs with minimal settings. See "License Information" for a list of the features that are always available. Contact RealNetworks or your reseller to purchase an updated license.

Look in the error log for messages.

RealProxy's error log (a text file named `proxy.log` or `proxy`, and located in the Logs directory) may contain a message describing the nature of the problem.

Step 2: Follow the network routing.

If there are any obstacles in the route that RealSystem packets take as they move through the network, RealProxy may not be able to contact other RealSystem components, such as RealPlayers and RealServers.

There are two general areas to check:

- Whether RealProxy can receive from the transmitter RealServer
- Whether a client can receive content from RealProxy

RealProxy-to-RealServer Connections

Before investigating any client-to-RealProxy issues, be sure the RealProxy-to-RealServer connections are working properly.

Problems may be related to:

- The transmitter RealServer is no longer broadcasting or is unable to broadcast any clip.
- The administrator of the transmitter RealServer has disabled access to all RealProxys, or has blocked access of your RealProxy in particular.
- The transmitter RealServer is incorrectly configured for pull splitting.
- A firewall is blocking access. See Chapter 7, “Firewalls and RealProxy” for more information.

On the RealProxy machine, use the method described in “Using TELNET to Test Connections” to ensure that the connection between RealProxy and RealServer is clear.

Client-to-RealProxy Connections

- Make sure clients are able to connect to RealProxy.
- Make certain there aren’t any access control rules on RealProxy that prohibit the client from receiving any broadcast or stream.
- If RealProxy is using multicast to distribute the stream inside the network, look for multicast user list rules that insist that the client receive the broadcast in multicast mode. If the client is not configured for multicast reception, it will not be able to receive the broadcast. See Chapter 11, “Multicasting Live Streams” for more information.

On the RealProxy machine, use the method described in "Using TELNET to Test Connections" to ensure that the connection between the client and RealProxy is clear.

Using TELNET to Test Connections

Instructions in this section describe how to use the TELNET program to determine whether a TCP connection exists between two computers. This information is often the first step in figuring out where the problem lies.

If the TELNET program is able to make a successful connection between computers, the problem is not a routing one. Use the troubleshooting guidelines in this chapter to work out a solution.

If the program is not able to make a successful connection, the problem is either a simple configuration issue on the other computer, or it may be a network routing problem.

➤ To use TELNET to test connections between the client and RealProxy:

1. Open a TELNET session.
2. At the `telnet>` prompt, type the following command:

   ```
   telnet>open realproxy.example.com port
   ```

   where:

   realproxy.example.com is the name of the machine on which RealProxy is running

   port is either of the ports below:

   Port Numbers for Client-to-RealProxy Connections

Port	Purpose
554	RTSP proxy requests
1090	PNA proxy requests

3. The response indicates your next step.

Telnet Information for Client-to-RealProxy Connections

TELNET Response	Significance

`Trying 172.23.16.123...`
`Connected to` *`realserver.example.com`*`.`
`Escape character is '^'.`
	RealProxy is listening on the port you specified. Use troubleshooting steps in this chapter.

`Trying 172.23.16.123...`
`telnet: Unable to connect to remote host:`
`Connection refused`
	RealProxy is not listening on the port specified. Access control rules may be in effect. Or, RealProxy may not be binding properly to its addresses.

`Trying 172.23.16.123...`
`telnet: Unable to connect to remote host:`
`No route to host`
	RealProxy's host computer is unreachable. Make sure there is a network connection to the RealProxy.

`realserver.example.com``: Unknown host`
`or`
`realserver.example.com``: Host name lookup failure`
	The other computer does not exist, or the host name cannot be resolved by the local DNS server.

➤ **To use TELNET to test connections between RealProxy and the transmitter:**

1. Open a TELNET session.
2. At the `telnet>` prompt, type the following command:

```
telnet>open realserver.example.com port
```

where:

realproxy.example.com is the name of the machine on which RealProxy is running

port is the number of the port number you are testing.

Port Numbers for RealProxy-to-RealServer Connections

Port	Purpose
554	Control channel for RTSP requests (data channel also, if TCP was requested)
3030	Data channel for pull splitting requests
7070	Control channel for PNA requests (data channel also, if TCP was requested)
7878	RealProxy requests for data by the cache

3. The response indicates your next step.

Telnet Information for RealProxy-to-RealServer Connections

TELNET Response	Significance

`Trying 172.23.16.123...`
`Connected to` *`host.domain`*`.`
`Escape character is '^'.`
	The transmitter is listening on the port you specified. Use troubleshooting steps in this chapter.

`Trying 172.23.16.123...`
`telnet:  Unable to connect to remote host:  Connection refused`
	The transmitter is not listening on the port specified.
	Access control rules may be in effect. Or, the transmitter may not be binding properly to its addresses.

`Trying 172.23.16.123...`
`telnet:  Unable to connect to remote host:  No route to host`
	The transmitter is unreachable.

`host.domain``:  Unknown host`
`or`
`host.domain``:  Host name lookup failure`
	Either you are typing an incorrect address, or the transmitter does not exist.

Step 3: Ensure that clients are configured correctly.

Be sure that client software is configured to connect to RealProxy. Refer to Chapter 5, "Connecting Clients to RealProxy".

Step 4: Check remaining areas.

Read further in this chapter for help with specific features.

- Is the RealProxy host machine address correctly configured in the network routers? If the client cannot access RealProxy over the network, then you cannot expect media to play. Configuring IP address and routers is a complex issue. Contact a networking specialist for help.
- Is there a firewall between the client and RealProxy? Firewalls must be configured to permit media to play through them. See Chapter 7, "Firewalls and RealProxy".
- Is there a parent RealProxy in use? If it is misconfigured, all clients may have difficulty receiving streams. Make sure the parent RealProxy can make the necessary connections to the RealServer. See Chapter 10, "Proxy Routing".

Step 5: Work with your system or network administrator.

Others in your organization may have information you need, such as available port numbers, or information on bandwidth restrictions.

Troubleshooting RealSystem Administrator

How do I figure out which port number to use for RealSystem Administrator?

1. Using a text editor, open the configuration file, which is named `rmserver.cfg` and is located in the main RealProxy directory, and search the file for `AdminPort`.
2. You will find an entry similar to the following (your port number will be different):

   ```
   <Var AdminPort="7845"/>
   ```

   Make a note of the number.
3. In your Web browser, type the following, substituting your computer's IP address for *address* and the number you found for *AdminPort* in the previous step:

   ```
   http://address:AdminPort/admin/index.html
   ```
4. RealSystem Administrator asks you for your user name and password. Type these and click OK.

   RealSystem Administrator appears.

How do I look up my user name and password?

When you install RealProxy, the setup program asks you for a user name and a password. It uses these for RealSystem Administrator and for any content creators who use G2 encoding software to send material to your RealProxy.

If you can't remember your password, you must reinstall RealProxy, or contact RealNetworks Technical Support department (see "Contacting RealNetworks Technical Support").

I can't start RealSystem Administrator.

- Make sure RealProxy is running. RealSystem Administrator cannot start if RealProxy is not running.

- You may need to add an IP Bindings section. Refer to “Binding to a Specific Address”.
- Be certain you are using the name of the machine that’s running RealProxy in the URL. Do not use a NetBIOS name; use the host name or the IP address, instead.
- Use the correct browser version. RealSystem Administrator is designed to run with Netscape 4.06 or higher, and Internet Explorer 4.01 or higher.
- If it was running before, and you have recently created new access control rules, you may have locked yourself out of the administrator. You will need to create a new rule, by editing the configuration file, that allows access to RealSystem Administrator. See “Creating Rules” for an explanation of the necessary rules.

I receive Javascript errors.

Javascript errors are usually due to an older browser version or the wrong version of RealProxy for your operating system. RealSystem Administrator is designed to run with Netscape 4.06 or higher, and Internet Explorer 4.01 or higher.

Troubleshooting Pull Splitting

Steps involved in troubleshooting pull splitting fall into two general areas:

- Whether RealProxy can receive from the transmitter RealProxy
- Whether a client can receive a split stream from RealProxy

If pull splitting is disabled on the transmitter RealProxy, your RealProxy will not be able to serve the clip via pull splitting. It will use passthrough mode for that clip.

Transmitter-to-RealProxy Connections

Before investigating any RealProxy-to-client issues, be sure the transmitter-to-RealProxy connections are working properly.

Problems with splitting may be related to:

- The transmitter RealServer is no longer broadcasting or is unable to broadcast any clip.

- The transmitter RealServer administrator has disabled pull splitting. This is unlikely, and the feature is enabled by default.
- The transmitter RealServer has blocked your RealProxy's access.

You can test the connection by connecting a client to the transmitter RealServer to make sure the clip exists and is being broadcasted; use a client from a machine that is not routed through RealProxy.

RealProxy-to-Client Connections

Make sure that RealProxy can receive a regular unicast from the transmitter RealServer. If unicasting is not working, splitting will not work, either.

Make certain there aren't any access control rules on RealProxy that prohibit the client from receiving any broadcast or stream.

If RealProxy is using multicast to distribute the split broadcast inside the network, look for multicast user list rules that insist that the client receive the broadcast in multicast mode. If the client is not configured for multicast reception, it will not be able to receive the broadcast.

Messages that contain the phrase "bit save" refer to pull splitting.

- "Warning - No split mount point has been defined. Bit save playback will not be supported."
- "Warning - RTSP proxy discarding message from server, data playback occurring from live splitter."
- "Warning - RTSP proxy is detecting redundant splitter challenges."

Troubleshooting Multicasting

Before setting up multicasting, two conditions must exist:

- RealProxy must be licensed for multicasting
- The network must be set up for multicasting

If these two conditions have been met, use the following information to troubleshoot this feature.

Steps in troubleshooting multicasting fall into two areas:

- Running the multicast on RealProxy
- Connecting to the multicast with a client

Checking RealProxy

The following error messages, appearing in the error log, indicate either that you have configured a back-channel multicast in RealSystem Administrator with **Delivery Only** set to `Yes` (`DeliveryOnly=True` in the configuration file):

- "Multicast delivery only"
- "This server is configured to support only multicast connections. Please contact the content provider for more information on listening to this broadcast."

The message "Error in creating Back-channel multicast session. Please increase the AddressRange configuration variable." indicates that RealProxy needs more multicast addresses in order to broadcast in back-channel multicast mode. In RealSystem Administrator, use a larger range in the IP Address Range boxes.

Special Issues with the Configuration File

If you configure back-channel multicast by editing the configuration file directly, you may inadvertently omit required sections. Without a ControlList section, multicasting will not work. Add it, using the format shown in "Multicasting Configuration Elements", or use RealSystem Administrator to set up the Client Access List. The error message that appears if this section is missing is:

- "Back-channel multicast is enabled and the control list is empty. No clients will receive multicast. Please add a control list."

If you make changes to the multicasting section of the configuration file, and you make those changes incorrectly, the following error messages may appear in the error log:

- "Warning - Proxy detects that the multicast address range provided is invalid. Check the configuration file."
- "Warning - Proxy cannot determine the IP multicast address range. Check the configuration for proper entry and/or syntax."

Use RealSystem Administrator to configure multicasting. You may need to check with your network administrator to find out the correct address range to use for your network.

Connecting with the Client

Try to play the clip from the same system on which RealProxy is installed.

Problems with multicasting may be related to:

- The network or the client is not multicast-enabled.
- Access control rules prohibit client from receiving any broadcast or stream.
- Multicast user list rules insist that the client receive the broadcast in multicast mode, and the client is not configured for multicast reception.

Troubleshooting Access Control

In addition to the required rules, make sure you have at least three rules, so that you can continue to connect to RealSystem Administrator, as described in"Creating Rules" .

The first rule to create is always the rule that allows you to access RealSystem Administrator! If you create another rule first, and lock yourself out of RealSystem Administrator, you will need to edit the configuration file, remove the rule manually, and then restart RealProxy. See "Access Control" for a guide on what to look for in the configuration file.

If you receive the message, "Invalid player IP Address", it is because this RealProxy is configured with access rules that prevent clients from certain IP addresses from playing content. The client that tried to request content is excluded via access rules. Access rules are described in Chapter 9, "Limiting Access to RealProxy".

Troubleshooting Caching

If you edit the configuration file directly to configure this feature, you risk accidentally deleting a key section. If you delete the cache mount point information, the following error message appears:

- "Warning - Proxy can not find the cache mount point. Proxy will fall to pass-through."

Set up the cache information using RealSystem Administrator.

Troubleshooting Proxy Routing

This feature is described in Chapter 10, "Proxy Routing".

Make certain that only the child RealProxy has been configured. The parent RealProxy receives the child's requests automatically, and requires no settings to do this. If the parent has been configured to send its requests to another RealProxy, and no such RealProxy is available, clients will display error messages.

If only some requests are being honored, and you have checked that the parent RealProxy has not been configured at all, make sure the child's list of rules includes a broad rule that handles all requests not specified in the other rules.

Contacting RealNetworks Technical Support

If you have followed the troubleshooting tips in this chapter and have not been able to solve the problem, check the RealNetworks Knowledge Base for help. The Knowledge Base contains solutions to many problems not covered here:

- **http://service.real.com/kb/default.htm**

For technical support with RealSystem, please fill out the form at:

- **http://service.real.com/contact/email.htm**

The information you provide in this form will help technical support personnel to give you a prompt response. For general information about RealNetworks' technical support, visit:

- **http://service.real.com/help/call.html**

In addition asking for a detailed description of the problem you are experiencing, support technicians will want to know the information shown in the following form.

> **Note**
>
> Space for noting information about RealServer is included for those customers who are also running RealServer on their networks.

Information Needed by the RealNetworks Technical Support Department

	RealProxy	RealServer
	Information About Your Software	
Exact Server version (see "Determining the RealProxy Version")	8._._._ _ _	8._._._ _ _
Information About Your System		
Operating system		
Processor type and speed		
Available RAM		
Port numbers		
Type of connection to the Internet		
Is there a Web server on this system?		
	Information About Other Software	
Client software version		
Encoding software version		
	Information About the Problem	
Exact text of error message (if any):		
How are you delivering content—are you streaming on-demand clips or broadcasting live clips?		
To how many clients are you streaming simultaneously?		
If the problem is with a certain feature, when was the last time it worked correctly? What has changed?		
Are there any related problems?		
What features are you using?		
What troubleshooting steps have you already tried?		

Determining the RealProxy Version

There are two methods for finding the exact version of RealProxy you are running.

➤ To determine the version of RealProxy (at a command prompt):

At a command prompt, navigate to the `Bin` directory, and type the following:

```
rmserver -v
```

The version number appears, in the form `8.`*x*`.`*x*`.`*xxx*, where *x* varies according to your operating system.

➤ To determine the version of RealProxy (through RealSystem Administrator):

In RealSystem Administrator, click **About**.

A new browser window appears, with information about your Server.

The version number can vary according to the operating system you use. If you are contacting the RealNetworks Technical Support department for assistance, it is important that they know the exact version you have.

Note

If you are also using a RealServer, these same steps can be used to determine the version of RealServer.

Appendix A

CONFIGURATION FILE SYNTAX

This appendix describes the structure of the configuration file.

Configuration File Components

The configuration file is constructed entirely of tags. There are four types of tags in this file: the XML declaration tag, optional comment tags, list tags, and variable tags.

Of these four types, only two make up the instructions to RealProxy: lists and variables. Lists are used for instructions that have several parts, such as the MIME types or the multicast instructions. A list tag is followed by one or more list tags or variable tags.

All values for lists and variables are enclosed in double quotation marks.

XML Declaration Tag

The XML declaration tag indicates which version of XML is in use. RealProxy uses XML version 1.0. The declaration tag looks like this:

```
<?XML Version="1.0" ?>
```

Comment Tags

Comment tags are used in the configuration file to identify the functions of tags, but the comments aren’t required. XML comment tags are just like those in HTML: they begin with <!-- and end with -->. RealProxy ignores these tags; they are for your benefit.

For example, this comment tag lets the administrator know that the parameters after it refer to the path settings:

```
<!-- P A T H S -->
```

Tip

To disable a feature, convert the feature's tag or tags to a comment. Rather than converting each tag to a comment, edit only the feature's first opening tag and last closing tag.

Do not nest comment tags within other comment tags.

List Tags

The list tag uses the following syntax:

```
<List Name="name">

...

</List>
```

where *name* is the list title. Using the correct capitalization for *name* is important.

Other lists or variables follow the list. The `</List>` tag signifies the end of the list. If other lists are inside the original list, they must also have closing `</List>` tags. The `MIMETypes` list is an example of a list that contains other lists.

Tip

Indenting list items is not required, but is recommended for clarity.

Variable Tags

Variable tags use the following syntax:

```
<Var name="value"/>
```

where *name* is the variable title, and *value* is a string or a number, depending on the variable. Capitalization for both *name* and *value* is important.

Unlike lists, variables do not have a closing tag; instead, a forward slash mark (/) appears before the closing angle bracket (>).

Tip

If you've restarted RealProxy and it's not responding to a change you've made to a variable, make sure the variable has a closing forward slash mark, and that there is no space between them.

Variables can be independent elements (such as `LogPath`) or they may appear inside a list. When variables appear within a list, their meaning is determined by the value of the list name, although they may be apparently identical in syntax to variables that are not inside lists. If there are multiple variables within a list that do similar things, their names must be unique. For example, the `Extension` variables within each `MIMETypes` list must have different names; this is accomplished by adding a number to the end of each (`Extension_01`, `Extension_02`, and so on).

Appendix B

CONFIGURATION FILE CONTENTS

This appendix gives brief information about the contents of the configuration file for those administrators interested in editing it directly.

Editing the Configuration File

For those RealProxy administrators who prefer to modify features by editing the configuration file directly, this appendix shows sample configuration file contents with brief descriptions. Detailed descriptions can be found in the chapters that describe each subject.

If you are going to modify the configuration file directly, please read the following sections:

- **Appendix A, "Configuration File Syntax"**—explains the structure of this file
- **"Configuring RealProxy Features" in Chapter 4**—contains instructions on modifying the configuration file with a text editor

It is recommended that you first use RealSystem Administrator to make changes, and then examine the configuration file to learn how changes are made. Noticing how lists are created and changed will be especially instructive.

Warning

Exit RealSystem Administrator before opening the configuration file with a text editor or unexpected changes may result.

Elements of the Configuration File

Settings are grouped into like categories. Variables that are not part of lists can appear anywhere in the configuration file, but are grouped here for clarity.

Most configuration file variables closely match names in RealSystem Administrator. Differences are noted here.

Access Control

Restricting access to RealProxy content via the requesting client's IP address is described in Chapter 9, "Limiting Access to RealProxy". For every address or address range to which you want to restrict access, create a list with a unique number. The number can be any length, but a number of more than one digit is recommended in case more lists are added later; with multiple digits, the new lists can be inserted between existing lists.

Each list is called a rule. Rules are processed in numerical order. RealProxy searches the list of rules to find the first rule that matches the address. Because RealProxy searches the list of rules in numerical order, make your broadest categories first.

Within each list, the following settings are used: `Access`, `Transport`, `To`, `From`, and a list named `Ports`.

Access Control Configuration Elements

Element	Description
`<List Name="AccessControl">`	
`  <List Name="0">`	This is a permanent rule. It permits access to RealProxy from an application running on the same computer. Do not modify or delete this rule.
`    <Var Access="Allow"/>`	Whether access is allowed or denied: set to `Allow` or `Deny`.
`    <Var From="localhost"/>`	Address of the host RealProxy or network card of hosting machine. Use specific address or `Any`.
`    <Var To="any"/>`	Address of the client computer whose access you are limiting. Use specific address or `Any`. To specify a range of IP addresses, either place a colon after the IP address and give the full subnet mask, or place a slash mark after the IP address and give the number of bytes for the subnet mask. For example, the following are equivalent values to use in the `From` variable: `172.16.3.0:255.255.255.0` and `172.16.3.0/24`. Both examples specify the range of addresses from 172.16.3.0 to 172.16.3.254.

Access Control Configuration Elements (continued)

Element	Description
<List Name="Ports">	List of ports to which access is restricted.
<Var Port_01="any"/>	Specific port number, or use the word any.
</List>	
</List>	
<List Name=”1”>	This is a permanent rule. It prevents other computers from accessing ports 6060 and 7070, which are reserved for RealProxy’s use. Do not modify or delete this rule.
<Var Access=”Deny”/>	See description earlier in this section.
<Var From=”any”/>	See description earlier in this section.
<Var To=”any”/>	See description earlier in this section.
<List Name=”Ports”>	See description earlier in this section.
<Var Port_1=”6060”/>	These ports are used exclusively by RealProxy.
<Var Port_2=”7070”/>	
</List>	
</List>	
<List Name=”2”>	You may add new rules here, but the rule shown here as Rule 2 must always appear last on the list. Insert other rules above this one, and give this one a new number.
<Var Access=”Allow”/>	See description earlier in this section.
<Var From=”any”/>	See description earlier in this section.
<Var To=”any”/>	See description earlier in this section.
<List Name=”Ports”>	See description earlier in this section.
<Var Port_1=”any”/>	See description earlier in this section.
</List>	
</List>	
</List>	

Authentication

Authentication is used to verify the identity of users. This feature is described in Chapter 12, “Authenticating RealProxy Users”.

Authentication

This section associates each realm with a database.

Authentication Realms Configuration Elements

Element	Description
<List Name="ProxyAuthentication">	
<Var Enabled=”1”/>	Indicates that authentication is enabled. 0 turns off this feature.
<List Name="Authority">	A realm.
<Var Realm="example.com. ConnectRealm"/>	Name of this realm.
<Var AllowDuplicateIDs=”1”/>	When set to 1, allows users to log in from more than one location.
</List>	
<List Name=”RuleList”>	List of rules and associated characteristics.
<List Name=”Rule1”>	
<Var NoAuthenticateHost= ”*.example.com”/>	
</List>	
<Var PluginID=”rn-auth-basic”/>	Security type.
<Var DatabaseID=”Connect_RN5”/>	Database name.
</List>	
</List>	
</List>	

Authentication Realms

This list highlights the realms and the associated databases.

Authentication Realms Configuration Elements

Element	Description
<List Name="AuthenticationRealms">	
<List Name="SecureAdmin">	A realm.
<Var Realm="AdminRealm"/>	Name of this realm.
<List Name=”BasicAuthenticator”/>	Type of authentication.
<Var PluginID=”rn-auth-basic”/>	Security type.
<Var DatabaseID=”Admin_Basic”/>	Database name.
</List>	
</List>	
<List Name="ConnectRealm">	Authentication information for connection authentication.
<Var Realm="ConnectRealm"/>	See description above.
<List Name="BasicAuthenticator">	
<Var PluginID="rn-auth-basic"/>	
<Var DatabaseID="Connect_RN5"/>	
</List>	
</List>	

Databases List

The databases list stores user names and passwords of authorized users.

Within the list, sublists associate database plugins with location information.

The options available to each sublist are `PluginID`, `Path`, `DBName`, `DBLoginPassword`, and `DBLoginPassword`. The last two are only required if the `PathToDBPlugin` is set to `ppvm3260` or `ppvo3260`.

Databases Configuration Elements

Element	Description
<List Name="Databases">	
<List Name="Admin_Basic">	Authentication of RealSystem Administrator users.

Databases Configuration Elements (continued)

Element	Description
<Var PluginID="rn-db-flatfile"/>	Name of plugin that will interact with the database.
<Var Path="C:\Program Files\Real \RealProxy\adm_b_db"/>	Location where the database files are stored or will be stored.
</List>	
<List Name=”Connect_RN5”>	Authentication of user connections.
<Var PluginID=rn-db-flatfile”/>	Name of plugin that will interact with the database.
<Var Path=”C:\Program Files\Real\ RealProxy\con_r_db”/>	Lcation of database files.
</List>	
</List>	

Caching

This feature is described in “Media Cache”.

There are two cache sections within the FSMount list: the cache file system and the local file system.

Within the cache file system section, the following variables are used: ShortName, MountPoint, and CacheShortName.

Caching Configuration Elements

Element	Description
<List Name=”FSMount”>	
...	
<List Name=”RealSystem Cache Filesystem”>	
<Var ShortName=”pn-mii-mgr”/>	Name of the plug-in manager.
<Var MountPoint=”/cachemgr/”/>	Name of the mount point (used internally)
<Var CacheShortName=”rn-cache”/>	Short name to use.
</List>	
<List Name=”RNCache Local File System”>	
<Var ShortName=”pn-local”/>	Uses local file system.
<Var MountPoint=”/fsforcache/”/>	Name of the mount point (used internally)

Caching Configuration Elements (continued)

Element	Description
`<Var BasePath="C:\RealProxy\Cache"/>`	Location of cached files.
`</List>`	
...	
`</List>`	
`<List Name="RNCache">`	
`<Var Enabled="1"/>`	Turns on the use of cache.
`<Var MaxCacheSizeMB="1000"/>`	Gives maximum size of cache storage, in megabytes.
`<Var CacheMountPoint="/fsforcache/"/>`	Name of the mount point (used internally)
`</List>`	

File Systems

The `FSMount` section of the configuration file gives the names of all the configurable file system plug-ins in use. The plug-ins themselves are stored in a directory indicated by the `PluginDirectory` variable. All requests of the RealProxy are processed by plug-ins.

ShortName Variable

Each list within `FSMount` gives a short name for the plug-in. The short name is also stored within the plug-in file itself, and RealProxy uses this to identify the correct file to use. The short name is referenced with the `ShortName` variable in each file systems list.

Local File System

The RealSystem Content list is used for internal processes by RealProxy.

RealSystem Administrator

Two files systems work together to operate RealSystem Administrator: the local file system and the administration file system.

The administration file system accepts the initial URL for RealSystem Administrator. It requests the HTML files from the local file system. Once the local file system delivers the HTML files, the administration file system looks up your RealProxy's values and displays them at the appropriate points in RealSystem Administrator.

Three variables are used for the RealAdministrator list: ShortName, MountPoint, and BasePath.

Five variables are use in the RealAdministrator_Files list: ShortName, MountPoint, Authorized_User_Group, Authentication, and Realm.

This tool is described in Chapter 4, "Configuring RealProxy Features".

RealSystem Administrator Configuration Elements

Element	Description
<List Name="RealSystem Administrator Files">	
<Var ShortName="pn-admin">	RealSystem Administrator uses the pn-admin plugin.
<Var MountPoint="/admin/"/>	The default value for MountPoint is /admin/. If you change this, you will need to type a new URL to connect to RealSystem Administrator.
<Var BaseMountPoint="/localadmin/"/>	This special form of mount point reflects the mount point of the RealAdministrator list.
<Var Realm="AdminRealm"/>	The Realm variable identifies which AuthenticationRealm settings will be used with requests sent to the RealSystem Administrator mount point.
<Var Authentication="True"/>	Indicates that authentication is in use.
</List>	
<List Name="RealAdministrator">	
<Var ShortName="pn-local"/>	RealSystem Administrator uses the local file system.
<Var MountPoint="/localadmin/"/>	Mount point, used when RealAdministrator_Files list requests files from this plugin. The default value is /localadmin/. If you change this, be sure to change the RealAdministrator_Files list's BaseMountPoint to match.
<Var BasePath="C:\Program Files \Real\RealProxy\RealAdministrator"/>	Location of the RealSystem Administrator files.
</List>	

RealSystem Administrator Configuration Elements (continued)

Element	Description
`<List Name=”RealSystem Administrator HTML”>`	This list defines the file system, mount point, and location of the files used by RealSystem Administrator.
`<Var ShortName=”pn-local”/>`	
`<Var MountPoint=”/admin/html/”/>`	
`<Var BasePath=”/RealAdministrator”/>`	
`</List>`	
`<List Name=”RealSystem Administrator DOCS”>`	Location for the online documentation for this product.
`<Var ShortName=”pn-local”/>`	
`<Var MountPoint=”/admin/Docs/”/>`	
`<Var BasePath=”/RealAdministrator/Docs”/>`	
`</List>`	
`<List Name=”RealSystem Administrator IMAGES”>`	This list gives the location where RealSystem Administrator can find the images to display on its pages.
`<Var ShortName=”pn-local”/>`	
`<Var MountPoint=”/admin/images/”/>`	
`<Var BasePath=”/RealAdministrator /images”/>`	
`</List>`	
`<List Name="RealSystem Administrator SSI">`	Server-side include handler; creates HTML pages in RealSystem Administrator.
`<Var ShortName="pn-xmltag"/>`	
`<Var MountPoint="/admin/includes/"/>`	
`<Var BaseMountPoint="/admin/html/"/>`	
`<List Name="TagHandlers">`	
`<Var h1="pn-includer"/>`	
`</List>`	
`</List>`	

Splitter Broadcast

This section is described in “Splitting”.

HTTP Support

This feature, which indicates the virtual directories whose content can be streamed via HTTP, is explained in Chapter 9, "Limiting Access to RealProxy". Each `Path` variable gives the name of a virtual directory whose content can be streamed via HTTP.

Be sure that `Admin` is on this list; `Admin` refers to RealSystem Administrator, which is served via HTTP. And push splitting uses HTTP for the initial connection conversation; add the push splitting mount point to this list, usually `farm`.

HTTP Deliverable Configuration Elements

Element	Description
`<List Name="HTTPDeliverable">`	
`  <Var Path_1="/admin"/>`	Each `Path` variable gives the name of a mount point, directory or virtual directory whose content can be streamed via HTTP.
`</List>`	

IP Bindings

The ability to run on specific addresses is explained in Chapter 6, "Advanced Features". This list uses variables numbered sequentially: `Address_01`, `Address_02`, and so on. Use one for each IP address you want to set aside for RealProxy. Use the RealProxy's IP address or host name for each variable; however, the IP address allows RealProxy to be more efficient.

RealProxy will bind to the specified addresses only; it will not bind to localhost.

If you don't use any values for the variables in the `IPBindings` list, RealProxy binds to the host IP address and localhost. It does not bind to any others.

IP Binding Configuration Elements

Element	Description
`<List Name="IPBindings">`	

IP Binding Configuration Elements (continued)

Element	Description
`<Var Address_01="0.0.0.0"/>`	Each variable gives an address to reserve for use by RealProxy. If using individual addresses, include `127.0.0.1` (loopback address). To reserve all addresses, use `0.0.0.0` and no others.
`</List>`	

Logging

Logging and reporting features are described in Chapter 14, "Tracking RealProxy Activity". Variables which control the locations of the access and error log files are described in "Paths" of this chapter.

Logging Configuration Elements

Element	Description
`<Var LoggingStyle=”5”/>`	Determines how much data about clips served is gathered in the access log. See Chapter 14, "Tracking RealProxy Activity" for a list of options.
`<Var LogRollFrequency="4W"/>`	Creates a new access log for each period specified. The period is indicated in the format `xD`, `xW`, or `xM`, where `x` is a number. See also `LogRollSize`. For example, `4D` will keep 4 days of information in the log file.
`<Var LogRollSize="50"/>`	Creates a new access log when the indicated file size is reached. See also `LogRollFrequency`. If you include both `LogRollFrequency` and `LogRollSize`, RealProxy uses the variable it finds first.
`<Var DisableClientGUID="0"/>`	Collects unique client identifiers ("GUIDs"). When set to 1, ignores all client GUIDs and uses `00000000-0000-0000-0000-000000000000` instead. Refer to "Omitting Client Identifiers".

Disable log file rolling by changing the `LogRollFrequency` and `LogRollSize` variables to `0`.

MIME Types

This section can only be edited via the configuration file.

MIME Types Configuration Elements

Element

```
<List Name="MimeTypes">
  <List Name="audio/x-pn-realaudio">
    <Var Ext_1="ram"/>
  </List>
  <List Name="image/gif">
    <Var Ext_1="gif"/>
  </List>
  <List Name="image/jpg">
    <Var Ext_1="jpg"/>
    <Var Ext_2="jpeg"/>
  </List>
  <List Name="text/html">
    <Var Ext_1="html"/>
    <Var Ext_2="htm"/>
  </List>
</List>
```

Multicasting

Back-channel multicasting is described in Chapter 11, “Multicasting Live Streams”.

Settings used with this list are `AddressRange`, `DeliveryOnly`, `RTSPPort`, `Resend`, and `TTL`.

Multicasting Configuration Elements

Element	Description
`<List Name="Multicast">`	
`<Var AddressRange="`*address-address*`"/>`	Range of addresses to which you want to send streams, in the form of *address-address*. RealProxy uses the first available address in this range. If you are using other types of multicast, be sure that the address ranges are different and do not overlap. If your multicast streams are referenced in SMIL files, you will need one address for each stream.
`<List Name="ControlList">`	The `ControlList` list gives the addresses of clients allowed to receive multicast transmissions.

Multicasting Configuration Elements (continued)

Element	Description
`<Var Allow="164.16.2.24:255.0.0.0"/>`	Address and netmask, separated by a colon, of clients allowed to receive multicast transmissions. Uses same format as `From` variable in `AccessControl` list.
`</List>`	
`<Var DeliveryOnly="False"/>`	Requires clients listed in `ControlList` to receive only multicast transmissions from RealProxy. When `DeliveryOnly` is `False`, clients on `ControlList` can receive both multicasts and unicasts.
`<Var RTSPPort="554"/>`	Port on client machines to which RealProxy sends RTSP streams. Default value is `554`.
`<Var TTL="16"/>`	Time To Live for multicast packets travelling over the network.
`<Var Resend="True"/>`	Allows or denies requests from clients for resends of missing UDP packets.
`</List>`	

Passwords

MonitorPassword is described in Chapter 13, “Monitoring RealProxy Activity”.

Password Configuration Elements

Element	Description
`<Var MonitorPassword="letmein"/>`	Password used by G2 Java Monitor in connecting to RealProxy.

Paths

`LogPath` and `ErrorLogPath` are described in Chapter 14, “Tracking RealProxy Activity”. `PIDPath` is described in Chapter 6, “Advanced Features”. `PluginDirectory` is described in Chapter 4, “Configuring RealProxy Features”. `LicenseDirectory` is given in Chapter 3, “Starting and Stopping RealProxy”.

Windows Variables

Path variables, along with typical paths used in Windows NT and Windows NT, are shown here.

Path Configuration Elements

Element	Description
`<Var LogPath="C:\Program Files\Real \RealProxy\Logs\proxy.log"/>`	`LogPath` indicates where and with what name the proxy log will be stored. If omitted, RealProxy places `proxy.log` in the `Logs` directory.
`<Var ErrorLogPath="C:\Program Files\Real \RealProxy\Logs\proxyerr.log"/>`	`ErrorLogPath` gives the path and name of the error log file. If this setting is omitted, RealProxy places `proxyerr.log` in the `Logs` directory.
`<Var PluginDirectory="C:\Program Files\Real \RealProxy\Plugins"/>`	Shows where the plug-in files are stored.
`<Var LicenseDirectory="C:\Program Files\Real \RealProxy\License"/>`	Gives the location of the license files.
`<Var SupportPluginDirectory=”C:\Program Files \Real\RealProxy\Lib”/>`	Shows location of the `Lib` directory

UNIX Variables

One additional setting is found on RealProxy running on a UNIX system: `PIDPath`.

Path Configuration Elements

Element	Description
`<Var LogPath="/usr/bin/RealProxy/Logs /proxy.log"/>`	`LogPath` indicates where and with what name the proxy log will be stored. If omitted, RealProxy places `proxy.log` in the `Logs` directory.
`<Var ErrorLogPath="/usr/bin/RealProxy/Logs /proxyerr.log"/>`	`ErrorLogPath` gives the path and name of the error log file. If this setting is omitted, RealProxy places `proxyerr.log` in the `Logs` directory.
`<Var PluginDirectory="/usr/bin/RealProxy /Plugins"/>`	Shows where the plug-in files are stored.
`<Var LicenseDirectory="/usr/bin/RealProxy /License"/>`	Gives the location of the license files.
`<Var PidPath="/usr/bin/RealProxy/Logs /rmserver.pid"/>`	In UNIX systems, the location of the process id file.

Path Configuration Elements (continued)

Element	Description
`<Var SupportPluginDirectory="/usr/bin /RealProxy/Lib"/`	Shows location of the `Lib` directory

Ports

Port settings are described in Chapter 4, "Configuring RealProxy Features". `MonitorPort` is described in Chapter 13, "Monitoring RealProxy Activity".

Ports Configuration Elements

Element	Description
`<Var MonitorPort="9090"/>`	The port which monitors (such as G2 Java Monitor) connect to RealProxy.
`<Var AdminPort="7845"/>`	Port number for RealSystem Administrator connection, randomly generated at setup.
`<Var HTTPPort=”8080”/>`	The port to which HTTP requests are made.
`<Var RTSPPort=”6060”/>`	Internal ports used by RealProxy to communicate with its file systems. External access to these ports is restricted.
`<Var PNAPort=”7070”/>`	

Proxy Routes Table

This feature is described in Chapter 10, "Proxy Routing".

Proxy Routes Table Configuration Elements

Element	Description
`<List Name="ProxyRouteTable">`	
`  <List Name="100">`	Rule number.
`    <Var Rule="*.tokyo.example.com"/>`	All Tokyo traffic is allowed to go to the Tokyo server, without being forwarded to a parent RealProxy.
`    <Var ParentMEIPort="7878"/>`	Caching port number on parent RealProxy.
`    <Var ParentPNAPort="7070"/>`	PNA port number of parent RealProxy.
`    <Var ParentRTSPPort="554"/>`	RTSP port number of parent RealProxy.

Proxy Routes Table Configuration Elements (continued)

Element	Description
`<Var ParentName=""/>`	Address of parent RealProxy.
`<Var UseParentProxy="0"/>`	Enables use of this feature.
`</List>`	
`<List Name="200">`	See description earlier in this section.
`<Var Rule="*"/>`	
`<Var ParentRTSPPort="554"/>`	
`<Var ParentMEIPort="7878"/>`	
`<Var ParentPNAPort="7070"/>`	
`<Var UseParentProxy="1"/>`	
`<Var ParentName= "realproxy.example.com"/>`	All traffic not specified in the previous rule will be forwarded to a parent RealProxy named realproxy.example.com.
`</List>`	
`</List>`	

RealProxy

If you establish values for `MaxProxyConnections`, `MaxProxyBandwidth`, and `MaxGatewayBandwidth`, RealProxy will limit access when the lowest threshold is reached.

RealProxy Configuration Elements

Element	Description
`<!-- P R O X Y  S E R V E R-->`	
`<List Name="Proxy">`	
`<Var RTSPPort=”554”/>`	Port number where RealProxy listens for RTSP requests.
`<Var PNAPort=”1090”/>`	Port number where RealProxy listens for PNA requests.

RealProxy Configuration Elements (continued)

Element	Description
`<Var CacheEnable="1"/>`	When value is `1`, RealProxy looks for media cache information in the configuration file and forwards requests for on-demand material to the cache file system. (See the “Caching” section in this chapter.) Enabled at installation.
`<Var CacheMountPoint=”/cachemgr/”/>`	Identifies the mount point to use for caching.
`<Var BitsaveEnable="1"/>`	When value is `1`, RealProxy streams all live requests, rather than opening separate data channels between the transmitter and the client. If you disable this setting, RealProxy will not be able to perform pull splitting.
`<Var BitsaveMountPoint=”/split/”/>`	Mount point automatically added to links in pull splitting mode.
`<Var BitsavePort=”3030”/>`	Corresponds to the port used in pull splitting.
`<Var MaxProxyConnections="0"/>`	Limits the number of connections that RealProxy will proxy simultaneously. Must be less than or equal to the number of streams in your license. Range is `1` to `32767`. If omitted or set to `0`, no limit is enforced.
`<Var MaxProxyBandwidth="0"/>`	Limits the amount of kilobits per second which RealProxy will use overall. This is not a per-connection setting. If omitted or set to `0`, no limit is enforced.
`<Var MaxGatewayBandwidth=”0”/>`	Limits the bandwidth in kilobits per second that RealProxy will use when connecting to its gateway. If omitted or set to `0`, no limit is enforced.
`</List>`	

Splitting

Only three variables are required in the pull splitting section: `ShortName`, `MountPoint`, and `Port`.

If the proxy routing feature is in use, two additional variables are used: `ParentProxyAddress`, and `ParentProxyPort`. The proxy routing feature is described in Chapter 10.

This section is part of the `FSMount` list.

Warning

If you change these settings, RealProxy will not be able to operate in pull splitting mode.

Pull Splitting Configuration Elements

Element	Description
`<List Name="Splitter_DoubleURL">`	
`<Var ShortName="pn-splitter"/>`	Short name of the pull splitting plugin. Default is `pn-splitter`.
`<Var MountPoint="/split/"/>`	Mount point. Used in URLs that reference pull splitting streams. Default is /split/.
`<Var Port="3030"/>`	Port number to which the transmitter will listen for pull splitting requests.
`<Var SplitterProtocol="UDP"/>`	Shows which type of protocol the transmitter will use to transmit data to the receiver. Choose `TCP` if you are splitting through a firewall (but this will produce a slower connection and more overhead).
`</List>`	

UNIX-Only Settings

These settings are also described in “Features Specific to the Operating System”.

UNIX-Only Configuration Elements

Element	Description
`<Var Group="users"/>`	Group name under which RealProxy runs. The group name must already exist on the computer on which RealProxy is running; otherwise, RealProxy will not start. If you do not specify a group name, this variable defaults to the group name of the user who first starts RealProxy. The default value is `%-1`.

UNIX-Only Configuration Elements (continued)

Element	Description
`<Var User="canderson"/>`	User name under which RealProxy runs. The user name must exist on the computer on which RealProxy is running; otherwise, RealProxy will not start. If you don't specify a user name during Setup, the user name defaults to the user name of the user who first logs in and starts RealProxy. The default value is `%-1`.
`<Var ProcessorCount="0"/>`	The default value of `0` means that RealProxy will use its test to determine the number of processors available. If you have more than one processor on your system, you should change this variable.

Features Only Available Via Direct Editing

Some of the more specialized lists and variables are only configurable by editing the configuration file directly; they cannot be changed via RealSystem Administrator.

These elements are:

- Most settings that would affect the use of RealSystem Administrator, such as the file systems used by the various RealSystem Administrator components.
- Short names of plug-ins, which most users are unlikely to change.
- Platform-specific variables, such as those described in "UNIX Variables""UNIX-Only Settings" (Group and User).
- MIME types. See "MIME Types".
- `LicenseDirectory` variable, which tells RealServer where to look for the license key file. Described in "Paths".
- `MonitorPassword` variable, the password used by RealSystem Administrator in connecting to the G2 Java Monitor. Described in "Passwords".
- `PluginDirectory` variable; gives the location of the `Plugin` directory. See "Paths".
- `SupportPluginDirectory` variable; gives the location of the `Lib` directory. See "Paths".

INDEX